開發人員指南

# AWS Config

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Config: 開發人員指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 AWS Config？ ..... 1
考量事項 ..... 1
使用方式 AWS Config ..... 1
資源管理 ..... 1
稽核與合規性 ..... 2
組態變更的管理和故障診斷 ..... 2
安全分析 ..... 2
合作夥伴解決方案 ..... 2
功能 ..... 2
如何 AWS Config 工作 ..... 3
資源探索 ..... 4
資源追蹤 ..... 4
配置項目的交付 ..... 5
控制存取 AWS Config ..... 7
概念 ..... 8
AWS Config 介面 ..... 9
資源管理 ..... 9
組態記錄器 ..... 10
交付通道 ..... 5
AWS Config 規則 ..... 11
一致性套件 ..... 13
彙總工具 ..... 14
區域支援 ..... 15
服務配額 ..... 19
AWS 服務整合 ..... 20
AWS Organizations ..... 20
AWS Control Tower ..... 21
AWS CloudTrail ..... 21
AWS Security Hub ..... 21
AWS Audit Manager ..... 21
AWS Systems Manager ..... 21
AWS Firewall Manager ..... 22
Amazon EC2 專用執行個體 ..... 22
Application Load Balancer ..... 22

AWS CodeBuild ... 23
AWS X-Ray ... 23
AWS Service Management Connector ... 23
Amazon API Gateway ... 23
補充資訊 ... 23
AWS 軟體開發套件 AWS Config ... 24
開始使用 ... 26
註冊成為 AWS ... 26
註冊一個 AWS 帳戶 ... 26
建立具有管理權限的使用者 ... 26
開始使用的方法 AWS Config ... 28
設定 AWS Config (主控台) ... 28
設定 ... 28
一鍵式設定 ... 29
手動設定 ... 31
設定 AWS Config (AWS CLI) ... 37
設定 ... 37
必要條件 ... 38
開始 AWS Config ... 97
驗證 ... 106
使用 AWS 軟體開發套件 ... 107
組態記錄器 ... 109
管理組態記錄器 (主控台) ... 109
管理組態記錄器 (AWS CLI) ... 110
組態記錄器的漂移偵測 ... 113
交付通道 ... 114
術語 ... 114
更新交付管道 ... 115
重新為交付管道命名 ... 118
組態項目的元件 ... 120
交付組態快照 ... 121
提供組態快照 ... 121
範例組態快照來源 AWS Config ... 122
驗證交付狀態 ... 127
檢視 Amazon S3 儲存貯體中的組態快照 ... 128
範例通知 ... 129

範例組態項目變更通知 ..... 130
範例組態歷史記錄交付通知 ..... 144
範例組態快照交付已啟動通知 ..... 145
範例組態快照交付通知 ..... 146
範例合規性變更通知 ..... 147
範例規則評估已啟動通知 ..... 150
範例大型組態項目變更通知 ..... 151
範例交付失敗通知 ..... 152
資源管理 ..... 154
AWS Config 儀表板 ..... 154
合規性與資源庫存 ..... 155
AWS Config 使用狀況和成功量度 ..... 156
支援的資源類型 ..... 158
Amazon AppStream ..... 159
Amazon AppFlow ..... 159
..... 160
Amazon API Gateway ..... 160
Amazon Athena ..... 160
Amazon CloudFront ..... 161
Amazon CloudWatch ..... 161
Amazon CodeGuru ..... 162
Amazon Cognito ..... 163
Amazon Connect ..... 163
Amazon Detective ..... 164
Amazon DynamoDB ..... 164
Amazon EC2 ..... 164
Amazon ECR ..... 172
Amazon ECS ..... 172
Amazon EFS ..... 173
Amazon EKS ..... 173
Amazon EMR ..... 174
Amazon EventBridge ..... 174
Amazon Forecast ..... 175
Amazon Fraud Detector ..... 176
Amazon GuardDuty ..... 176
Amazon Inspector ..... 177

Amazon IVS ..... 177
Amazon Keyspaces ..... 177
Amazon OpenSearch 服務 ..... 178
Amazon Personalize ..... 178
Amazon Pinpoint ..... 179
Amazon QLDB ..... 180
Amazon Kendra ..... 180
Amazon Kinesis ..... 180
Amazon Lex ..... 181
Amazon Lightsail ..... 182
Amazon Lookout for Metrics ..... 182
Amazon Lookout for Vision ..... 182
Amazon Managed Grafana ..... 183
Amazon Managed Service for Prometheus ..... 183
Amazon MemoryDB for Redis ..... 183
Amazon MQ ..... 183
Amazon MSK ..... 184
Amazon Redshift ..... 184
Amazon RDS ..... 186
Amazon Route 53 ..... 187
Amazon SageMaker ..... 188
Amazon SES ..... 189
Amazon SNS ..... 190
Amazon SQS ..... 190
Amazon S3 ..... 190
Amazon WorkSpaces ..... 192
AWS Amplify ..... 192
AWS AppConfig ..... 193
AWS App Runner ..... 194
AWS App Mesh ..... 194
AWS AppSync ..... 195
AWS Audit Manager ..... 195
AWS Auto Scaling ..... 195
AWS Backup ..... 196
AWS Batch ..... 197
AWS Budgets ..... 198

AWS Certificate Manager ..... 198
AWS CloudFormation ..... 198
AWS CloudTrail ..... 198
AWS Cloud9 ..... 199
AWS Cloud Map ..... 199
AWS CodeArtifact ..... 200
AWS CodeBuild ..... 200
AWS CodeDeploy ..... 200
AWS CodePipeline ..... 201
AWS Config ..... 201
AWS DMS ..... 202
AWS DataSync ..... 203
AWS Device Farm ..... 204
AWS Elastic Beanstalk ..... 205
AWS FIS ..... 205
AWS Global Accelerator ..... 206
AWS Glue ..... 206
AWS Ground Station ..... 207
AWS HealthLake ..... 207
AWS IAM ..... 207
AWS IoT ..... 209
AWS KMS ..... 212
AWS Lambda ..... 213
AWS Mainframe Modernization ..... 213
AWS Network Firewall ..... 213
AWS Network Manager ..... 214
AWS Panorama ..... 215
AWS Private CA ..... 215
AWS Resilience Hub ..... 216
AWS 資源總管 ..... 216
AWS RoboMaker ..... 217
AWS Signer ..... 217
AWS Secrets Manager ..... 217
AWS Service Catalog ..... 218
AWS Shield ..... 218
AWS Step Functions ..... 219

AWS Systems Manager ..... 219
AWS Transfer Family ..... 220
AWS WAF ..... 220
AWS X-Ray ..... 222
Elastic Load Balancing ..... 222
MediaConnect ..... 223
MediaPackage ..... 224
MediaTailor ..... 224
依區域可用性列出的資源涵蓋範圍 ..... 225
北美洲和南美洲 ..... 225
歐洲 ..... 285
亞太區域 ..... 334
中國 ..... 382
非洲和中東 ..... 416
GovCloud ..... 464
錄製 AWS 資源 ..... 508
考量事項 ..... 508
區域和全球資源 ..... 508
記錄資源（主控台） ..... 511
錄製AWS CLI 資源 ..... 514
記錄頻率 ..... 529
停止記錄 ..... 530
非記錄資源 ..... 530
AWS Config 規則和全域資源類型 ..... 530
記錄第三方資源 ..... 531
步驟 1：設定您的開發環境 ..... 532
步驟 2：建立資源模型 ..... 532
步驟 3：產生成品 ..... 534
步驟 4：註冊您的資源 ..... 535
步驟 5：發佈資源組態 ..... 535
使用記錄和刪除協力廠商資源的組態狀態 AWS CLI ..... 535
使用 API 管理第三方資源類型的組態狀態 ..... 538
錄製軟體組態 ..... 538
檢視已記錄的 資源 ..... 540
資源庫存 ..... 541
合規資訊與評估結果 ..... 542

組態與符合性歷程記 ... 554
為您的資源建立標籤 ... 563
標記相關的限制 ... 563
以 AWS Config API 動作管理標籤 ... 564
AWS Config 規則 ... 565
成本考量 ... 566
區域支援 ... 567
規則的元件 ... 572
規則中繼資料 ... 572
規則結構 ... 574
評估模式 ... 591
觸發類型 ... 591
評估模式 ... 592
規則評估 ... 595
受管規則 ... 596
成本考量 ... 566
觸發類型 ... 597
評估模式 ... 598
受管規則清單 ... 598
依評估模式排序的受管規則清單 ... 883
按觸發類型排序的受管規則清單 ... 899
依區域可用性列出的受管規則清單 ... 914
服務連結規則 ... 1251
使用AWS CloudFormation範本建立受管規則 ... 1251
自訂規則 ... 1253
自訂政策規則 ... 1253
自訂 Lambda 規則 ... 1253
成本考量 ... 566
觸發類型 ... 1254
評估模式 ... 1255
管理已刪除的資源 ... 1256
建立自訂政策規則 ... 1257
建立自訂 Lambda 規則 ... 1260
新增、更新及刪除規則 ... 1290
使用主控台 ... 1290
使用 AWS 軟體開發套件 ... 1296

使用 Security Hub ..... 1307
使用 規則評估資源 ..... 1308
刪除評估結果 ..... 1312
刪除評估結果 (主控台) ..... 1312
刪除評估結果 (CLI) ..... 1312
刪除評估結果 ..... 1312
管理組織規則 ..... 1313
考量事項 ..... 1313
部署 ..... 1314
區域支援 ..... 1314
修補 ..... 1316
先決條件 ..... 1317
設定手動修補 (主控台) ..... 1317
設定自動修補 (主控台) ..... 1318
刪除修補動作 (主控台) ..... 1319
管理修補 (API) ..... 1320
區域支援 ..... 1320
故障診斷 ..... 1324
一致性套件 ..... 1326
必要條件 ..... 1326
開始 AWS Config 錄製 ..... 1326
使用一致性套件搭配修補的先決條件 ..... 1327
將符合性套件與一或多個規則搭配使用的先決條件 AWS Config ..... 1327
組織一致性套件的先決條件 ..... 1330
區域支援 ..... 1332
程序檢查 ..... 1336
用於建立程序檢查的一致性套件範例範本 ..... 1337
在一致性套件內包含程序檢查 ..... 1337
變更程序檢查的合規狀態 ..... 1338
檢視和編輯程序檢查 (主控台) ..... 1339
一致性套件範例範本 ..... 1339
AWSControl Tower Detective 護衛合規包 ..... 1343
ABS CCIG 2.0 重大工作負載的操作最佳實務 ..... 1344
ABS CCIG 2.0 標準工作負載的操作最佳實務 ..... 1480
ACSC Essential 8 的操作最佳實務 ..... 1579
ACSC ISM 的操作最佳實務 ..... 1595

AI 和 ML 的操作最佳實務 ..... 1679
Amazon API Gateway 的操作最佳實務 ..... 1679
Amazon 的操作最佳實踐 CloudWatch ..... 1679
Amazon DynamoDB 作最佳實務 ..... 1680
Amazon S3 的操作最佳實踐 ..... 1680
APRA CPG 234 的操作最佳實務 ..... 1680
資產管理的操作最佳實務 ..... 1818
AWS Backup的操作最佳實務 ..... 1818
AWS身分識別與存取管理的營運最佳作法 ..... 1818
AWS Well-Architected 架構可靠性支柱的營運最佳實務 ..... 1818
Well-Architec AWS ted 的架構安全性支柱的營運最佳實務 ..... 1854
BCP 和 DR 的操作最佳實務 ..... 1959
BNM RMiT 的操作最佳實務 ..... 1959
加拿大網路安全中心 (CCCS) 中型雲端控制設定檔的最佳營運實務 ..... 2134
獨聯體 AWS 基金會基準 v1.4 級 1 的運營最佳實踐 ..... 3038
獨聯體 AWS 基金會基準第 1.4 版第 2 級的運營最佳實踐 ..... 3063
CIS Critical Security Controls v8 IG1 的操作最佳實務 ..... 3097
CIS Critical Security Controls v8 IG2 的操作最佳實務 ..... 3153
CIS Critical Security Controls v8 IG3 的操作最佳實務 ..... 3252
CIS 前 20 項的操作最佳實務 ..... 3359
CISA 網路基礎的操作最佳實務 ..... 3410
刑事司法資訊服務 (CJIS) 的操作最佳實務 ..... 3526
CMMC 第 1 級的操作最佳實務 ..... 3604
CMMC 第 2 級的操作最佳實務 ..... 3675
CMMC 第 3 級的操作最佳實務 ..... 3853
CMMC 第 4 級的操作最佳實務 ..... 4110
CMMC 第 5 級的操作最佳實務 ..... 4389
CMMC 2.0 第 1 級的操作最佳實務 ..... 4707
CMMC 2.0 第 2 級的操作最佳實務 ..... 4776
運算服務的操作最佳實務 ..... 5018
資料復原的操作最佳實務 ..... 5018
資料庫服務的操作最佳實務 ..... 5018
資料湖和分析服務的操作最佳實務 ..... 5018
DevOps 的操作最佳實務 ..... 5018
EC2 的操作最佳實務 ..... 5019
加密和金鑰管理的操作最佳實務 ..... 5019

ENISA 中小企業網路安全指南的操作最佳實務 ..... 5019
Esquema Nacional de Seguridad (ENS) Low 的操作最佳實務 ..... 5121
Esquema Nacional de Seguridad (ENS) Medium 的操作最佳實務 ..... 5189
Esquema Nacional de Seguridad (ENS) High 的操作最佳實務 ..... 5264
FDA 標題 21 CFR 操作最佳實務第 11 部分 ..... 5347
FedRAMP (低) 的操作最佳實務 ..... 5540
FedRAMP (適中) 的操作最佳實務 ..... 5699
FFIEC 的操作最佳實務 ..... 6030
德國雲端運算合規性標準目錄 (C5) 的最佳作業實務 ..... 6164
Gramm Leach Bliley Act (GLBA) 的操作最佳實務 ..... 6217
GxP EU Annex 11 的操作最佳實務 ..... 6245
HIPAA 安全的操作最佳實務 ..... 6332
IRS 1075 的操作最佳實務 ..... 6623
K-ISMS 的操作最佳實務 ..... 6743
負載平衡的操作最佳實務 ..... 6795
日誌的操作最佳實務 ..... 6796
管理與控管服務的操作最佳實務 ..... 6796
MAS Notice 655 的操作最佳實務 ..... 6796
MAS TRMG 的操作最佳實務 ..... 6821
監控的操作最佳實務 ..... 6964
NBC TRMG 的操作最佳實務 ..... 6964
NERC CIP BCSI 的操作最佳實務 ..... 7236
NCSC 雲端安全原則的操作最佳實務 ..... 7266
NCSC 網路評估架構的操作最佳實務 ..... 7331
聯網和內容交付服務的操作最佳實務 ..... 7440
NIST 800-53 修訂版 4 的操作最佳實務 ..... 7440
NIST 800-53 修訂版 5 的最佳操作實務 ..... 7628
NIST 800 171 的操作最佳實務 ..... 8103
NIST 800 172 的操作最佳實務 ..... 8308
NIST 800 181 的操作最佳實務 ..... 8348
NIST 1800 25 的操作最佳實務 ..... 8654
NIST CSF 的操作最佳實務 ..... 8756
NIST 隱私權架構 1.0 版的操作最佳實務 ..... 8979
NYDFS 23 的操作最佳實務 ..... 9126
NZISM 的操作最佳實務 ..... 9230
PCI DSS 3.2.1 的操作最佳實務 ..... 9281

可公開存取資源的操作最佳實務 ..... 9522
RBI 城市合作銀行 (UCB) 網路安全架構的操作最佳實務 ..... 9523
RBI MD-ITF 的操作最佳實務 ..... 9554
安全、身分及合規服務的最佳實務 ..... 9643
無伺服器的操作最佳實務 ..... 9644
儲存服務的操作最佳實務 ..... 9644
SWIFT CSP 的操作最佳實務 ..... 9644
Amazon Elastic Container Service (Amazon ECS) 的安全最佳實務 ..... 9666
Amazon Elastic File System (Amazon EFS) 的安全最佳實務 ..... 9666
Amazon Elastic Kubernetes Service (Amazon EKS) 的安全最佳實務 ..... 9666
Amazon 的安全最佳實踐 CloudFront ..... 9666
Amazon OpenSearch 服務的安全最佳實踐 ..... 9666
Amazon Redshift 的安全最佳實務 ..... 9667
Amazon Relational Database Service (Amazon RDS) 的安全最佳實務 ..... 9667
AWS Auto Scaling的安全最佳實務 ..... 9667
AWS CloudTrail的安全最佳實務 ..... 9667
AWS CodeBuild的安全最佳實務 ..... 9668
Amazon ECR 的安全最佳實務 ..... 9668
AWS Lambda的安全最佳實務 ..... 9668
AWS Network Firewall的安全最佳實務 ..... 9668
Amazon 的安全最佳實踐 SageMaker ..... 9668
AWS Secrets Manager的安全最佳實務 ..... 9669
AWS WAF的安全最佳實務 ..... 9669
具有修補動作的範例範本 ..... 9669
自訂一致性套件 ..... 9669
術語 ..... 9670
自訂範本 ..... 9670
部署您的自訂一致性套件 ..... 9674
一致性套件儀表板 ..... 9674
導覽一致性套件主頁 ..... 9674
進一步了解 ..... 9675
檢視合規歷史記錄 ..... 9675
檢視合規時間軸 ..... 9676
查詢合規歷史記錄 ..... 9676
部署一致性套件 (主控台) ..... 9678
使用範本部署一致性套件 ..... 9678

編輯一致性套件 ..... 9680
刪除一致性套件 ..... 9680
部署一致性套件 (AWS CLI) ..... 9680
部署一致性套件 ..... 9681
檢視一致性套件 ..... 9682
檢視一致性套件狀態 ..... 9683
檢視一致性套件合規狀態 ..... 9683
取得特定一致性套件的合規詳細資訊 ..... 9684
刪除一致性套件 ..... 9685
管理一致性套件 (API) ..... 9685
管理組織一致性套件 ..... 9686
考量事項 ..... 9686
部署 ..... 9687
區域支援 ..... 9687
故障診斷 ..... 9689
符合性套件的失敗狀態 ..... 9689
符合性套件中的懸置規則 ..... 9690
彙總工具 ..... 9693
使用案例 ..... 9693
術語 ..... 9694
如何彙總資料 ..... 9694
區域支援 ..... 9695
故障診斷 ..... 9698
彙總工具儀表板 ..... 9699
使用彙總工具儀板表 ..... 9699
合規儀表板 ..... 9702
庫存儀表板 ..... 9703
設定彙整 (主控台) ..... 9705
建立彙整工具 ..... 9705
編輯彙整工具 ..... 9707
刪除彙整工具 ..... 9707
設定彙整 (AWS CLI) ..... 9708
使用個別帳戶新增彙整 ..... 9708
使用 AWS Organizations 新增彙整工具 ..... 9710
註冊委派管理員 ..... 9711
檢視彙整 ..... 9713

編輯彙整工具 ..... 9714
刪除彙整工具 ..... 9716
授權彙整工具帳戶 (主控台) ..... 9716
考量事項 ..... 9716
新增彙整工具帳戶及區域的授權 ..... 9717
授權彙整工具帳戶的擱置中請求 ..... 9717
刪除現有彙總工具帳戶的授權 ..... 9718
授權彙整工具帳戶 (AWS CLI) ..... 9718
考量事項 ..... 9719
新增彙整工具帳戶及區域的授權 ..... 9719
刪除授權帳戶 ..... 9719
進階查詢 ..... 9721
功能 ..... 9721
查詢元件 ..... 9722
概要 ..... 9722
參數 ..... 9722
範例 ..... 9722
查詢範例 ..... 9723
範例關係查詢 ..... 9729
限制 ..... 9730
區域支援 ..... 9733
查詢編輯器 (主控台) ..... 9736
考量事項 ..... 9736
使用範 AWS 例查詢 ..... 9737
建立自訂查詢 ..... 9737
查詢編輯器 (AWS CLI) ..... 9738
考量事項 ..... 9738
查詢資源組態資料 ..... 9739
儲存查詢 ..... 9740
檢視所有儲存的查詢 ..... 9741
取得儲存查詢的詳細資訊 ..... 9742
刪除儲存的查詢 ..... 9742
自然語言查詢處理器 ..... 9742
考量事項 ..... 9743
使用自然語言查詢處理器進行查詢 ..... 9737
範例提示 ..... 9744

提供回饋 ... 9747
區域支援 ... 9748
刪除 資料 ... 9749
設定資料保留期 (主控台) ... 9751
安全 ... 9752
資料保護 ... 9752
加密傳輸中的資料 ... 9753
加密傳輸中的資料 ... 9753
身分和存取權管理 ... 9753
物件 ... 9754
使用身分驗證 ... 9754
使用政策管理存取權 ... 9757
如何與 IAM AWS Config 搭配使用 ... 9759
身分型政策範例 ... 9765
AWS 受管政策 ... 9781
IAM 角色的許可 ... 9918
更新 IAM 角色 ... 9922
Amazon S3 存儲桶的許可 ... 9923
KMS 金鑰的許可 ... 9927
Amazon SNS 主題的許可 ... 9930
故障診斷 ... 9933
使用服務連結角色 ... 9935
事件反應 ... 9936
合規驗證 ... 9937
恢復能力 ... 9938
基礎設施安全性 ... 9938
組態與漏洞分析 ... 9938
預防跨服務混淆代理人 ... 9939
最佳實務 ... 9939
記錄和監控 ... 9940
日誌 ... 9940
AWS Config 信息在 CloudTrail ... 9940
瞭解 AWS Config 記錄檔項目 ... 9941
範例日誌檔案 ... 9941
監控 ... 9949
使用 Amazon SQS ... 9949

使用 Amazon EventBridge ..... 9951
Amazon VPC 端點 ..... 9956
為以下項目建立 VPC 端點 AWS Config ..... 9956
常見問答集 ..... 9957
無法看到我最新的組態變更 ..... 9957
我可以預期立即檢視我的組態變更嗎？ ..... 9957
間接關係 AWS Config ..... 9957
什麼是資源關係？ ..... 9957
什麼是資源的直接和間接關係？ ..... 9958
哪些間接關係 AWS Config 支持？ ..... 9958
如何根據直接和間接關係建立組態項目？ ..... 9959
由於間接關係而產生的組態項目有哪些？ ..... 9960
如何擷取與間接關係相關的組態資料？ ..... 9961
程式碼範例 ..... 9963
動作 ..... 9963
DeleteConfigRule ..... 9964
DescribeComplianceByConfigRule ..... 9966
DescribeComplianceByResource ..... 9968
DescribeConfigRuleEvaluationStatus ..... 9969
DescribeConfigRules ..... 9971
DescribeConfigurationRecorderStatus ..... 9974
DescribeConfigurationRecorders ..... 9976
DescribeDeliveryChannels ..... 9977
GetComplianceDetailsByConfigRule ..... 9978
GetComplianceDetailsByResource ..... 9981
GetComplianceSummaryByConfigRule ..... 9983
GetComplianceSummaryByResourceType ..... 9984
PutConfigRule ..... 9986
PutDeliveryChannel ..... 9990
文件歷史記錄 ..... 9992
舊版更新 ..... 10080
..... 10133

# 什麼是 AWS Config？

AWS Config 提供您 AWS 帳戶中 AWS 資源組態的詳細檢視。這包含資源彼此之間的關係和之前的組態方式，所以您可以看到一段時間中組態和關係的變化。

AWS 資源是您可以在其中使用的實體 AWS，例如 Amazon Elastic Compute Cloud (EC2) 執行個體、Amazon Elastic Block Store (EBS) 磁碟區、安全群組或 Amazon Virtual Private Cloud (VPC)。如需支援的完整 AWS 資源清單 AWS Config，請參閱支援的資源類型。

## 考量事項

- AWS 帳戶：你需要一個積極的 AWS 帳戶。如需詳細資訊，請參閱註冊 AWS.
- Amazon S3 儲存貯體：您需要 S3 儲存貯體才能接收組態快照和歷史記錄的資料。如需詳細資訊，請參閱《Amazon S3 儲存貯體許可》。
- Amazon SNS 主題：當組態快照和歷程記錄發生變更時，您需要 Amazon SNS 才能接收通知。如需詳細資訊，請參閱 Amazon SNS 主題的許可。
- IAM 角色：您需要具有存取必要許可的 IAM 角色 AWS Config。如需詳細資訊，請參閱 IAM 角色的許可。
- 資源類型：您可以決定要 AWS Config 記錄的資源類型。如需詳細資訊，請參閱錄製 AWS 資源。

## 使用方式 AWS Config

在上執行應用程式時 AWS，通常會使用 AWS 資源，您必須共同建立和管理這些資源。隨著應用程式的需求不斷增加，您需要追蹤資 AWS 源也是如此。 AWS Config 旨在協助您在下列情況下監督應用程式資源：

### 資源管理

若要練習更恰當地管理資源組態，以及偵測不正確的資源組態，您需要微調資源的可見性，以及如何同時設定這些資源。您可 AWS Config 以使用在建立、修改或刪除資源時通知您，而不必透過輪詢對每個資源進行的呼叫來監視這些變更。

您可以使用 AWS Config 規則來評估 AWS 資源的組態設定。當 AWS Config 偵測到資源違反其中一個規則中的條件時，會將資源 AWS Config 標記為不相容並傳送通知。 AWS Config 在建立、變更或刪除資源時持續評估資源。

## 稽核與合規性

您可能處理需要頻繁稽核的資料，確保符合內部政策和最佳實務。若要示範合規性，您需要存取資源的歷史組態。此資訊由提供 AWS Config。

## 組態變更的管理和故障診斷

當您使用多個彼此相依的 AWS 資源時，變更一個資源的組態可能會對相關資源產生意外後果。使用 AWS Config，您可以檢視要修改的資源與其他資源的關係，並評估變更的影響。

您也可以使用 AWS Config 所提供資源的歷史組態對問題進行故障診斷，以及存取問題資源的上次已知正常組態。

## 安全分析

若要分析潛在的安全弱點，您需要有關資 AWS 源組態的詳細歷史資訊，例如授予使用者的 AWS Identity and Access Management (IAM) 許可，或控制資源存取權的 Amazon EC2 安全群組規則。

您可以隨時使用 AWS Config 檢視在其中記錄的使用者、群組或角色指派 AWS Config 的 IAM 政策。此資訊可協助您判斷在特定時間屬於使用者的許可：例如，您可以檢視使用者 `John Doe` 是否具有可在 2015 年 1 月 1 日修改 Amazon VPC 設定的許可。

您也可以使 AWS Config 用檢視 EC2 安全群組的組態，包括在特定時間開啟的連接埠規則。此資訊可協助您判斷安全群組是否封鎖傳入特定連接埠的 TCP 流量。

## 合作夥伴解決方案

AWS 與第三方專家合作進行記錄和分析，以提供使用 AWS Config 輸出的解決方案。如需詳細資訊，請造訪 AWS Config 詳細資訊頁面，網址為AWS Config。

# 功能

設定時 AWS Config，您可以完成以下操作：

資源管理

- 指定您要 AWS Config 記錄的資源類型。

- 設定 Amazon S3 儲存貯體於請求時接收組態快照及組態歷史記錄。

- 設定 Amazon SNS 傳送組態串流通知。
- 授予存 AWS Config 取 Amazon S3 儲存貯體和 Amazon SNS 主題所需的許可。

  如需詳細資訊，請參閱檢視 AWS 資源組態和歷程記錄和管理 AWS 資源組態與歷程記錄。

規則與一致性套件

- 指定您要用 AWS Config 來評估已記錄資源類型之符合性資訊的規則。
- 使用一致性套件或 AWS Config 規則和修正動作集合，這些動作可以在您的單一實體中部署和監視。AWS 帳戶

  如需詳細資訊，請參閱使用 AWS Config 規則與一致性套件評估資源。

彙總工具

- 使用彙總工具來集中檢視您的資源庫存和合規性。彙總器會將多個區 AWS 域和區域的 AWS Config 組態 AWS 帳戶 和合規性資料收集到單一帳戶和區域中。

  如需詳細資訊，請參閱《多帳戶多區域資料彙總》。

進階查詢

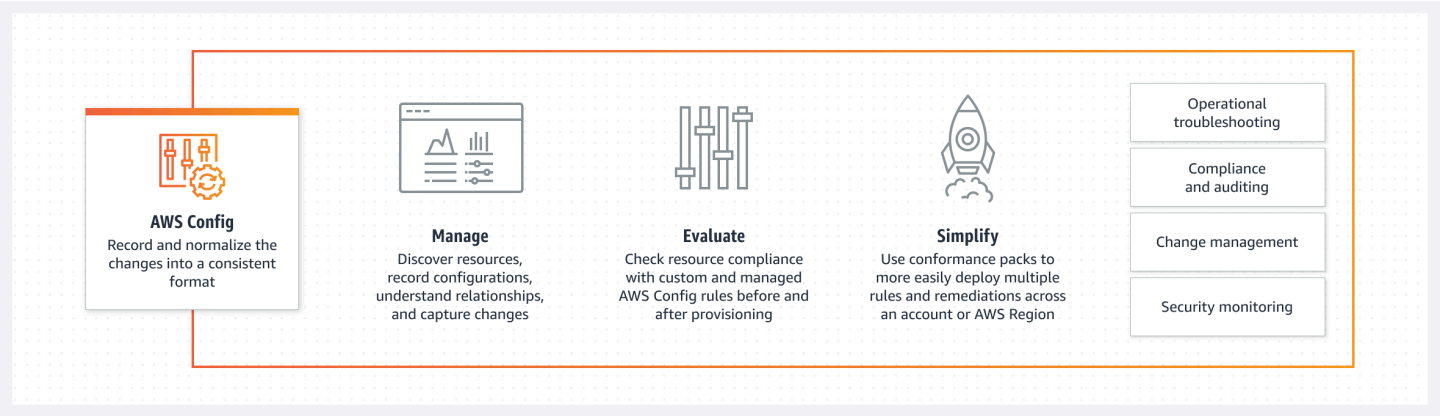
- 使用其中一個範例查詢，或參考 AWS 資源的組態結構描述來撰寫您自己的查詢。

  如需詳細資訊，請參閱查詢 AWS 資源的目前組態狀態。

# 如何 AWS Config 工作

AWS Config 提供您 AWS 帳戶中 AWS 資源組態的詳細檢視。這包含資源彼此之間的關係和之前的組態方式，所以您可以看到一段時間中組態和關係的變化。

AWS 資源是您可以在其中使用的實體 AWS，例如 Amazon Elastic Compute Cloud (EC2) 執行個體、Amazon Elastic Block Store (EBS) 磁碟區、安全群組或 Amazon Virtual Private Cloud (VPC)。如需支援的完整 AWS 資源清單 AWS Config，請參閱支援的資源類型。




## 資源探索

當您開啟時 AWS Config，它會首先探索您帳號中存在的支援 AWS 資源，並為每個資源產生一個組態項目。

AWS Config 當資源的組態變更時，也會產生組態項目，並在您啟動組態記錄程式時維護資源組態項目的歷史記錄。依預設， AWS Config 會為區域中每個受支援的資源建立組態項目。如果您不想 AWS Config 為所有支援的資源建立組態項目，您可以指定要追蹤的資源類型。

在指定 AWS Config 要追蹤的資源型態之前，請先勾選「依可用區域的資源涵蓋範圍」，以查看您要設定的「 AWS 區域」中是否支援資源型態 AWS Config。如果至少一個「區域」支援某個資源類型，則您可以 AWS Config 在所支援的所有「區域」中啟用該資源類型的記錄 AWS Config，即使指定的資源類型不支援您設定的「 AWS 區域」也一樣 AWS Config。

## 資源追蹤

AWS Config 透過為帳戶中的每個資源呼叫「描述」或「清單 API」呼叫來追蹤資源的所有變更。此服務使用這些相同的 API 呼叫來擷取所有相關資源的組態詳細資訊。

例如，從 VPC 安全性群組移除輸出規則會導致 AWS Config 在安全性群組上叫用「描述」API 呼叫。 AWS Config 然後在與安全群組相關聯的所有執行個體上叫用「描述 API」呼叫。安全群組 (資源) 和每個執行個體 (相關資源) 的已更新組態會記錄為組態項目，並以組態串流形式交付至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

AWS Config 也會追蹤 API 未啟動的組態變更。 AWS Config 定期檢查資源組態，並針對已變更的組態產生組態項目。

如果您使用的是 AWS Config 規則，請 AWS Config 持續評估您的 AWS 資源組態以取得所需的設定。根據規則， AWS Config 將評估您的資源，以回應組態變更或定期。每個規則都與 AWS Lambda 函數建立關聯，而此函數包含規則的評估邏輯。 AWS Config 評估資源時，它會叫用規則的 AWS Lambda

函數。該函數會傳回所評估資源的合規性狀態。如果資源違反規則的條件，則會將資源和規則 AWS Config 標記為不相容。當資源的合規狀態變更時， AWS Config 會傳送通知給您的 Amazon SNS 主題。

## 配置項目的交付

AWS Config 可透過下列其中一個管道遞送組態項目：

### Amazon S3 儲存貯體

AWS Config 追蹤 AWS 資源組態中的變更，並定期將更新的組態詳細資訊傳送到您指定的 Amazon S3 儲存貯體。對於 AWS Config 記錄的每個資源類型，它會每六個小時傳送一次組態歷程記錄檔案。每個組態歷史記錄檔案都會包含該六小時期間所變更資源的詳細資訊。每個檔案都會包含一種類型的資源 (例如 Amazon EC2 執行個體或 Amazon EBS 磁碟區)。如果沒有發生任何組態變更，則 AWS Config 不會傳送檔案。

AWS Config 當您將交付配置快照命令與 AWS CLI 搭配使用時，或將快照動作與 API 搭配使用時，會將組態快DeliverConfig照傳送到您的 Amazon S3 儲存貯體。 AWS Config 組態快照包含 AWS Config 記錄在您的 AWS 帳戶. 組態歷史記錄檔案和組態快照為 JSON 格式。

> **Note**
>
> AWS Config 只會將組態歷程記錄檔案和組態快照交付到指定的 S3 儲存貯體； AWS Config 不會修改 S3 儲存貯體中物件的生命週期政策。您可以使用生命週期政策，指定要刪除物件，還是將其封存至 Amazon S3 Glacier。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的管理生命週期組態。您也可以查看《將 Amazon S3 資料封存至 S3 Glacier》部落格文章。

### Amazon SNS 主題

Amazon Simple Notification Service (Amazon SNS) 主題是一種通訊頻道，Amazon SNS 運用該頻道來將訊息 (或通知) 交付至訂閱端點，例如電子郵件地址或用戶端。其他類型的 Amazon SNS 通知包含行動電話上傳送至應用程式的推播通知訊息、傳送至啟用 SMS 功能之行動電話和智慧型手機的簡訊服務 (SMS) 通知，以及 HTTP POST 請求。為了獲得最佳結果，請使用 Amazon SQS 作為 SNS 主題的通知端點，然後以程式設計方式處理通知中的資訊。

AWS Config 使用您指定的 Amazon SNS 主題傳送通知給您。您收到的通知類型會以訊息本文中 `messageType` 金鑰的值表示，如下列範例所示：

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

通知可以是下列任何一種訊息類型。

| 訊息類型 | Description |
| --- | --- |
| ComplianceChange通知 | AWS Config 評估之資源的符合性類型已變更。符合性類型會指出資源是否符合特定 AWS Config 規則，並以訊息中的`ComplianceType` 索引鍵表示。訊息包含要比較的 `newEvaluationResult` 和 `oldEvaluationResult` 物件。 |
| ConfigRulesEvaluationStarted | AWS Config 開始針對指定的資源評估規則。 |
| ConfigurationSnapshotDeliveryStarted | AWS Config 開始將組態快照交付到您的 Amazon S3 儲存貯體。已在訊息中為 `s3Bucket` 金鑰提供 Amazon S3 儲存貯體名稱。 |
| ConfigurationSnapshotDeliveryCompleted | AWS Config 成功地將組態快照交付到您的 Amazon S3 儲存貯體。 |
| ConfigurationSnapshotDeliveryFailed | AWS Config 無法將組態快照交付到您的 Amazon S3 儲存貯體。 |
| ConfigurationHistoryDeliveryCompleted | AWS Config 成功將組態歷史記錄交付到您的 Amazon S3 儲存貯體。 |
| ConfigurationItemChangeNotification | 已在組態中建立、刪除或變更資源。此訊息包含針對此變更所 AWS Config 建立之組態項目的詳細資訊，其中包含變更的類型。這些通知會在變更的數分鐘內交付，並且統稱為「組態串流」。 |
| OversizedConfigurationItemChange通知 | 組態項目變更通知超過 Amazon SNS 允許的大小上限時，會交付此訊息類型。訊息包含組態項目的摘要。除了 SMS 訊息外，Amazon SNS 訊息最多可包含 256 KB 的文字資料，包括 |

| 訊息類型 | Description |
| --- | --- |
| | XML、JSON 和未格式化的文字。您可以在指定的 Amazon S3 儲存貯體位置檢視完整通知。 |
| OversizedConfigurationItemChangeDeliveryFailed | AWS Config 無法將超大型組態項目變更通知傳送到您的 Amazon S3 儲存貯體。 |

如需範例通知，請參閱 AWS Config 傳送至 Amazon SNS 主題的通知。如需 Amazon SNS 的詳細資訊，請參閱 Amazon Simple Notification Service 開發人員指南。

> **Note**
>
> 為什麼我看不到最新的設定變更？
> AWS Config 通常會在偵測到變更之後或您指定的頻率，立即記錄資源的組態變更。但是，這是在最大努力的基礎上，有時可能需要更長的時間。如果問題在一段時間後仍然存在，請聯絡AWS Support並提供 Amazon 支援的 AWS Config 指標 CloudWatch。如需這些測量結果的相關資訊，請參閱AWS Config 使用狀況和成功測

## 控制存取 AWS Config

AWS Identity and Access Management 是一種網路服務，可讓 Amazon Web Services (AWS) 客戶管理使用者和使用者許可。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

  建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。
- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。

- (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

# 概念

AWS Config 提供與您相關聯之資源的詳細檢視 AWS 帳戶，包括如何設定資源、彼此之間的關聯性，以及組態及其關係在一段時間內如何變更。讓我們更詳細查看 AWS Config的概念。

內容


- AWS Config 介面
  - AWS Config 控制台
  - AWS Config CLI
  - AWS Config API
  - AWS Config 開發套件
- 資源管理
  - AWS 資源
  - 資源關係
- 組態記錄器
- 交付通道
  - 組態項目
  - 組態歷史記錄
  - 組態快照
  - 組態串流
- AWS Config 規則
  - AWS Config 受管規則
  - AWS Config 自訂規則
  - 觸發類型
  - 評估模式
- 一致性套件
- 多帳戶多區域資料彙整
  - 來源帳戶
  - 來源區域

- 彙整工具
- 彙整工具帳戶
- 授權

# AWS Config 介面

## AWS Config 控制台

您可以使用 AWS Config 控制台管理服務。如需有關的更多資訊 AWS Management Console，請參閱AWS Management Console。

## AWS Config CLI

這 AWS Command Line Interface 是一個統一的工具，您可以使用它 AWS Config 來從命令行進行交互。如需詳細資訊，請參閱 AWS Command Line Interface 使用者指南。如需 AWS Config CLI 命令的完整清單，請參閱可用的命令。

## AWS Config API

除了控制台和 CLI 之外，您還可以使用 AWS Config RESTful API AWS Config 直接進行編程。如需詳細資訊，請參閱 AWS Config API 參考。

## AWS Config 開發套件

作為使用 AWS Config API 的替代方法，您可以使用其中一個 AWS SDK。每種開發套件皆包含多種程式設計語言與平台的程式庫與範本程式碼。開發套件提供便捷方法來建立對 AWS Config的程式化存取。例如，您可以使用開發套件以密碼編譯方式來簽署請求、管理錯誤，以及自動重試請求。如需詳細資訊，請參閱 Amazon Web Services 適用工具頁面。

# 資源管理

瞭解的基本元件可協 AWS Config 助您追蹤資源清查與變更，並評估 AWS 資源的組態。

## AWS 資源

AWS 資源是您使用 AWS Command Line Interface (CLI) AWS Management Console、 AWS SDK 或 AWS 合作夥伴工具建立和管理的實體。 AWS 資源範例包括 Amazon EC2 執行個體、安全群組、Amazon VPC 和 Amazon 彈性區塊存放區。 AWS Config 指使用其唯一識別碼的每個資源，例如資源 ID 或 Amazon 資源名稱 (ARN)。如需 AWS Config 支援的資源類型清單，請參閱支援的資源類型。

### 資源關係

AWS Config 探索帳戶中的 AWS 資源，然後建立 AWS 資源之間關係的對映。例如，關係可能包含的 Amazon EBS 磁碟區 `vol-123ab45d`，其連接至與安全群組 `sg-ef678hk` 建立關聯的 Amazon EC2 執行個體 `i-a1b2c3d4`。

如需詳細資訊，請參閱 支援的資源類型。

## 組態記錄器

組態記錄器會將支援的資源組態當做組態項目存放在您的帳戶中。您必須先建立後啟動組態記錄器，才能開始記錄。您隨時可以停止和重新啟動組態記錄器。如需詳細資訊，請參閱 管理組態記錄器。

依預設，組態記錄程式會記錄執行所在區域中 AWS Config 的所有支援資源。您可以建立自訂組態記錄器，只記錄您指定的資源類型。如需詳細資訊，請參閱 錄製 AWS 資源。

如果您使用 AWS Management Console 或 CLI 來開啟服務， AWS Config 會自動為您建立並啟動組態錄製程式。

## 交付通道

隨著 AWS Config 持續記錄 AWS 資源發生的變更，它會透過傳遞通道傳送通知和更新的組態狀態。您可以管理傳遞通道，以控制 AWS Config 傳送組態更新的位置。

### 組態項目

組態項目代表您帳號中存在之受支援 AWS 資源的各種屬性的 point-in-time 檢視。組態項目的元件包括中繼資料、屬性、關係、目前的組態及相關事件。 AWS Config 每當它偵測到它正在記錄的資源類型的變更時，就會建立組態項目。例如，如果 AWS Config 要記錄 Amazon S3 儲存貯體，則每當建 AWS Config 立、更新或刪除儲存貯體時，都會建立組態項目。您也可以選擇為 AWS Config 以您設定的錄製頻率建立組態項目。

如需詳細資訊，請參閱 Components of a Configuration Item 和選取要記錄的資源 | 記錄頻率。

### 組態歷史記錄

組態歷史記錄是指定資源在任何時間期間的組態項目集合。組態歷史記錄可協助您回答下列這類問題，例如，第一次建立資源時、上個月如何設定資源，以及昨天 9 AM 進行何種組態變更。您可以使用多種格式的組態歷程記錄。 AWS Config 針對要記錄到您指定的 Amazon S3 儲存貯體的每個資源類型，自動交付組態歷史記錄檔案。您可以在 AWS Config 主控台中選取指定的資源，並使用時間軸瀏覽至該資源的所有先前設定項目。此外，您也可以從 API 存取資源的歷史組態項目。

如需詳細資訊，請參閱檢視 AWS 資源組態和歷程記錄和管理 AWS 資源組態與歷程記錄。

### 組態快照

組態快照是帳戶中現有所支援資源的組態項目集合。此組態快照是所記錄資源和其組態的完整全貌。組態快照可以是驗證組態的實用工具。例如，建議您定期檢查未正確設定或可能不存在之資源的組態快照。組態快照具有多種格式。您可以將組態快照交付至您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。此外，您可以在 AWS Config 主控台中選取時間點，並使用資源之間的關係瀏覽組態項目的快照集。

### 組態串流

配置流是一個自動更新的列表，其中包含 AWS Config 正在記錄的資源的所有配置項目。每次建立、修改或刪除資源時， AWS Config 都會建立組態項目，並新增至組態串流。使用您選擇的 Amazon Simple Notification Service (Amazon SNS) 主題後，組態串流即可運作。配置流有助於觀察發生的配置更改，以便您發現潛在問題，在某些資源發生變更時產生通知，或更新需要反映 AWS 資源配置的外部系統。

## AWS Config 規則

AWS Config 規則代表特定 AWS 資源或整個資源所需的組態設定 AWS 帳戶。如果資源未通過規則檢查，請將資源和規則 AWS Config 標記為不合規，然後透過 Amazon SNS 通 AWS Config 知您。以下是 AWS Config 規則可能的評估結果：

- `COMPLIANT` - 規則通過合規檢查的條件。
- `NON_COMPLIANT` - 規則未通過合規檢查的條件。
- `ERROR` - 其中一個必要/選用參數無效、類型不正確，或格式不正確。
- `NOT_APPLICABLE` - 用於篩選出無法套用規則邏輯的資源。例如，alb-desync-mode-check 規則僅檢查 Application Load Balancer，並忽略 Network Load Balancer 和 Gateway Load Balancer。

規則有兩種類型： AWS Config 受管規則和 AWS Config 自訂規則。如需有關規則定義和規則中繼資料結構的詳細資訊，請參閱AWS Config 規則的元件。

### AWS Config 受管規則

AWS Config 受管規則是由建立的預先定義、可自訂的規則 AWS Config。如需受管規則的清單，請參閱AWS Config 受管規則清單。

## AWS Config 自訂規則

AWS Config 自訂規則是您從頭開始建立的規則。建立 AWS Config 自訂規則的方法有兩種：使用 Lambda 函數 (AWS Lambda 開發人員指南)，以及使用 Guard (安全防護 GitHub儲存庫) (一種 policy-as-code 語言)。 AWS Config 使用建立的自訂規 AWS Lambda 則稱為AWS Config 自訂 Lambda 規則，而 AWS Config 使用安全警衛建立的自訂規則稱為AWS Config 自訂原則規則。

如需瞭解如何建立 AWS Config 自訂原則規則的逐步解說，請參閱建立 AWS Config 自訂原則規則。如需瞭解如何建立 AWS Config 自訂 Lambda 規則的逐步解說，請參閱建立 AWS Config 自訂 Lambda 規則。

### 觸發類型

將規則新增至帳戶後，請 AWS Config 將資源與規則條件進行比較。在此初始評估之後，每次觸發評估時都會 AWS Config 繼續執行評估。評估觸發程序被定義為規則的一部分，它們可以包括下列類型。

| 觸發類型 | Description |
| --- | --- |
| 組態變更 | AWS Config 當有符合規則範圍的資源，且資源的組態發生變更時，會執行規則的評估。評估會在 AWS Config 傳送組態項目變更通知後執行。<br><br>您可以透過定義規則的範圍來選擇要進行評估的資源。範圍可包含下列項目：<br><br>• 一或多個資源類型<br>• 資源類型和資源 ID 的組合<br>• 標籤鍵和值的組合<br>• 當任何記錄的資源建立、更新或刪除時<br><br>AWS Config 當偵測到符合規則範圍的資源變更時，會執行評估。您可以使用範圍來定義要進行評估的資源。 |
| 定期 | AWS Config 以您選擇的頻率執行規則的評估，例如，每 24 小時執行一次。 |

| 觸發類型 | Description |
| --- | --- |
| 混合 | 部分規則同時具有組態變更和定期觸發條件。對於這些規則，請在偵測到組態變更時以及您指定的頻率 AWS Config 評估您的資源。 |

## 評估模式

AWS Config 規則有兩種評估模式。

| 評估模式 | Description |
| --- | --- |
| 主動 | 使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是「非符合」(NON_COMPLUTION)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。 AWS<br><br>如需詳細資訊，請參閱《評估模式》。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。 |
| 偵測 | 使用偵測評估來評估已部署的資源。這可讓您評估現有資源的組態設定。 |

> **Note**
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

# 一致性套件

一致性套件是 AWS Config 規則與修正動作的集合，可輕鬆部署為帳戶和區域中的單一實體，或在中的組織中部署。 AWS Organizations

您可以透過編寫包含 AWS Config 受管或自訂規則和修補動作之清單的 YAML 範本，來建立一致性套件。您可以使用 AWS Config 主控台或 AWS CLI來部署範本。

若要快速開始使用並評估您的 AWS 環境，請使用其中一個範例一致性套件範本。您也可以根據《自訂一致性套件》，從頭開始建立一致性套件 YAML 檔案。自訂一致性套件是 AWS Config 規則和修正動作的唯一集合，您可以在帳戶和 AWS 區域中一起部署，或在中的組織中部署。 AWS Organizations

流程檢查是一種 AWS Config 規則類型，可讓您追蹤需要驗證作為一致性套件一部分的外部和內部任務。您可以將這些檢查新增至現有或新的一致性套件。您可以在單一位置追蹤所有合規性，包括 AWS Config排尿和手動檢查。

## 多帳戶多區域資料彙整

中的多帳戶多區域資料彙總 AWS Config 可讓您將來自多個帳戶和區域的 AWS Config 組態和合規性資料彙總到單一帳戶中。多帳戶多區域資料彙總對於中央 IT 管理員來說非常有用，以監控企業 AWS 帳戶 中的多個合規性。使用彙總工具不會產生任何額外費用。

### 來源帳戶

來源帳號是您要彙總 AWS Config 資源組態和符合性資料的來源帳號。 AWS 帳戶 來源帳戶可以是 AWS Organizations中的個別帳戶或組織。您可以個別提供來源帳戶，也可以透過擷取來源帳戶 AWS Organizations。

### 來源區域

來源區域是您要彙總 AWS Config 組態與合規性資料的 AWS 地區。

### 彙整工具

彙總器會從多個來源帳戶和區域收集 AWS Config 組態和符合性資料。在您要查看彙總 AWS Config 組態和合規性資料的區域中建立彙總工具。

> **Note**
>
> 彙總器透過將來源帳戶中的資料複寫到彙總器帳戶中，提供彙總器授權可檢視的來源帳戶和區域的唯讀檢視。彙總器不提供對來源帳戶或區域的變更存取權。例如，這表示您無法透過彙總器或推播快照檔案透過彙總器將規則部署到來源帳戶或區域。

### 彙整工具帳戶

彙整工具帳戶是您建立彙整工具的帳戶。

### 授權

身為來源帳戶擁有者，授權是指您授與彙總帳戶和區域的權限，以收集您的 AWS Config 組態和合規性資料。如果您要彙整屬於 AWS Organizations一部分的來源帳戶，則不需要授權。

## 區域支援

> **Note**
>
> 的 AWS Config 某些功能僅在支援的 AWS 區域的子集中 AWS Config 受支援。
>
> 資源管理
>
> - 如需「區域」支援哪些 AWS 資源型態的清單，請參閱依區域可用的資源涵蓋範圍。
>
> AWS Config 規則
>
> - 如需支援哪些區域的 AWS Config 規則清單，請參閱依區域可用性區域排序的 AWS Config 受管規則清單。
> - 如需 Support AWS Config 規則組織部署的區域清單，請參閱組織規則 | 地區支援。
> - 如需 Support AWS Config 規則修正動作的區域清單，請參閱修正動作 | 區域支援。
>
> 一致性套件
>
> - 如需支援一致性套件及一致性套件組織部署的區域清單，請參閱《一致性套件 | 區域支援。
>
> 彙整工具
>
> - 如需支援彙整工具的區域清單，請參閱《彙總工具 | 區域支援》。
>
> 進階查詢
>
> - 如需支援進階查詢的區域清單，請參閱《進階查詢 | 區域支援》。
> - 如需支援進階查詢之自然語言查詢處理器的區域清單，請參閱進階查詢的自然語言查詢處理器 | 區域支援。

下表列出了您可以啟用的 AWS 區域 AWS Config。

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com<br>config-fips.us-east-2.amazonaws.com | HTTPS<br>HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com<br>config-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com<br>config-fips.us-west-1.amazonaws.com | HTTPS<br>HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com<br>config-fips.us-west-2.amazonaws.com | HTTPS<br>HTTPS |
| 非洲 (開普敦) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| 亞太區域 (香港) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| 亞太區域 (海德拉巴) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (大阪) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 加拿大西部 (卡加利) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (米蘭) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (西班牙) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 歐洲 (蘇黎世) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| 以色列 (特拉維夫) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| 中東 (巴林) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| 中東 (阿拉伯聯合大公國) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# 服務配額

下表說明 AWS Config 內的限制。除非另有說明，否則可以在請求時提高配額。您可以要求增加配額。

如需 AWS 中其他限制的資訊，請參閱《AWS 服務限制》。

AWS Config Service Limits

| 描述 | 限制值 | 可以提高 |
| --- | --- | --- |
| 每個帳戶每個區域的 AWS Config 規則數上限 | 1000 | 否 |
| 每個資源的標籤數上限 | 50 | 否 |

單一帳戶一致性套件

| 描述 | 限制值 | 可以提高 |
| --- | --- | --- |
| 每個帳戶的一致性套件數量上限 | 50 | 否 |
| 每個一致性套件的 AWS Config 規則數上限 | 130 | 否 |

> **Note**
> 一致性套件中的 AWS Config 規則會計入每個區域每個帳戶的 AWS Config 規則數上限。

組織一致性套件

| 描述 | 限制值 | 可以提高 |
| --- | --- | --- |
| 每個組織的一致性套件數量上限 | 50 | 否 |
| 每個組織一致性套件的 AWS Config 規則數上限 | 130 | 否 |

> **Note**
>
> 在組織層級部署會計入子帳戶的限制。一致性套件中的 AWS Config 規則會計入每個區域每個帳戶的 AWS Config 規則數上限。

彙總工具

| 描述 | 限制值 | 可以提高 |
| --- | --- | --- |
| 組態彙總工具的數量上限 | 50 | 是 |
| 彙總工具中的帳戶數目上限 | 10000 | 否 |
| 所有彙總工具每週新增或刪除的帳戶數目上限 | 1000 | 是 |

進階查詢

| 描述 | 限制值 | 可以提高 |
| --- | --- | --- |
| 單一帳戶與區域中儲存的查詢數目上限 | 300 | 是 |

# AWS 與服務整合 AWS Config

AWS Config 支持與其他幾個 AWS 服務的集成。

## AWS Organizations

您可以使用 AWS Organizations 來定義要用於多帳戶、多區域資料彙總功能 AWS Config的帳戶。AWS Organizations 是一項帳戶管理服務，可協助您 AWS 帳戶 將多個組織整合到您建立並集中管理的組織中。透過提供 AWS Organizations 詳細資料，您可以監控整個組織的合規性狀態。若要取得更多資訊 AWS Config ， AWS Organizations請參閱《使AWS Organizations 用者指南》。

## AWS Control Tower

AWS Control Tower AWS Config 在所有註冊的帳號上啟用，以便它可以透過偵測控制來監視符合性、記錄資源變更，並將資源變更記錄傳遞至記錄封存帳戶。如需詳細資訊，請參閱《AWS Control Tower 使用指南》 AWS Config中的使用監視資源變更。

## AWS CloudTrail

AWS Config 與整合 AWS CloudTrail 以將組態變更與您帳戶中的特定事件相關聯。您可以使用 CloudTrail 記錄檔來取得呼叫變更的事件詳細資訊，包括提出要求的人員、在什麼時間，以及從哪個 IP 位址。您可以從 CloudTrail 主控台導覽至 AWS Config 時間軸，以檢視與 AWS API 活動相關的組態變更。

如需詳細資訊，請參閱AWS Config 開發人員指南 AWS CloudTrail中的使用記錄 AWS Config API 呼叫和AWS CloudTrail 使用使用者指南中的主控台為 AWS Config 設定項目建立事件資料存放區。

## AWS Security Hub

AWS Security Hub 集中從其他 AWS 服務（包括 AWS Config 規則）進行安全檢查。Security Hub 會啟用並控制 AWS Config 規則，以驗證您的資源組態是否符合最佳實務。在 Security Hub 所要 AWS Config 對環境資源執行安全性檢查的所有區域中的所有帳戶啟用。如需詳細資訊，請參閱AWS Security Hub 使用指南中的將發現項目傳送至 Security Hub 的AWS 服務。

## AWS Audit Manager

您可以使用 Audit Manager 來擷取 AWS Config 評估作為稽核的證據。當您建立或編輯自訂控制項時，您可以指定一或多個 AWS Config 規則作為證據收集的資料來源對應。 AWS Config 根據這些規則執行符合性檢查，「Audit Manager」會將結果報告為符合性檢查證據。如需詳細資訊，請參閱《AWS Audit Manager 使用指南》 AWS Audit Manager中的「支援的AWS Config 規則」。

## AWS Systems Manager

AWS Config 與 Systems Manager 整合，以記錄現場部署環境中 Amazon EC2 執行個體和伺服器上軟體的組態變更。透過這項整合，您可以瞭解作業系統 (OS) 組態、系統層級更新、已安裝的應用程式、網路組態等。 AWS Config 也提供作業系統和系統層級組態變更的歷史記錄，以及 Amazon EC2 執行個體記錄的基礎設施組態變更。您可以從 Systems Manager 主控台導覽至 AWS Config 時間表，以檢視受管 Amazon EC2 執行個體的組態變更。您可以使用 AWS Config 來檢視 Systems Manager 庫存歷史記錄，以及追蹤所有代管執行個體的變更。

如需詳細資訊，請參閱AWS Systems Manager 使用者指AWS Config 南中的與 AWS 服務整合 | 管理與控管、AWS Config 組態記錄程式和一致性套件部署。

## AWS Firewall Manager

若要使用 Firewall Manager 員，您必須 AWS Config 為每個成 AWS Organizations 員帳戶啟用。建立新應用程式時，Firewall Manager 是建置防火牆規則、建立安全性原則並一致強制執行這些規則的單一服務。如需詳細資訊，請參閱AWS WAF AWS Firewall Manager、和 AWS Shield Advanced 開發人員指南 AWS Config中的啟用。

> **Note**
>
> Firewall Manager 器取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。如需有關連續錄製和每日錄製的詳細資訊，請參閱錄製頻率。

## Amazon EC2 專用執行個體

AWS Config 與 Amazon EC2 專用主機整合，以評估授權合規性。 AWS Config 記錄在專用主機上啟動、停止或關閉執行個體的時間，並將此資訊與軟體授權相關的主機和執行個體層級資訊配對，例如主機 ID、Amazon Machine Image (AMI) ID、通訊端數量和實體核心。這有助於您 AWS Config 做為授權報告的資料來源使用。您可以從 Amazon EC2 專用主機主控台導覽至 AWS Config 時間表，以檢視 Amazon EC2 專用主機的組態變更。

如需詳細資訊，請參閱適用於 Linux 執行個體的 Amazon 彈性運算雲端使用者指南中的追蹤組態變更，或在 Amazon 彈性運算雲端 Windows 執行個體使用者指南中追蹤組態變更。

## Application Load Balancer

AWS Config 與 Elastic Load Balancing (ELB) 服務整合，以記錄對應用程式負載平衡器的組態變更。AWS Config 此外，還包括與相關聯的 Amazon EC2 安全群組、虛擬私人雲端和子網路的關係。您可以使用此資訊進行安全性分析和疑難排解。例如，您可以隨時檢查哪些安全群組與應用程式負載平衡器相關聯。您可以從 ELB 主控台導覽至 AWS Config 時間表，以檢視應用程式負載平衡器的組態變更。

## AWS CodeBuild

AWS Config提供您的 AWS 資源清單，以及這些資源的組態變更歷程記錄。 AWS Config 支持 AWS CodeBuild; 作為一種 AWS 資源，這意味著該服務可以跟踪您的 CodeBuild 項目。若要取得更多資訊，請參閱《使 AWS Config 用指南》中的AWS CodeBuild 與 CodeBuild 範例搭配使用

## AWS X-Ray

AWS X-Ray 與整合 AWS Config 以記錄對 X-Ray 加密資源所做的組態變更。您可以用 AWS Config 來清查 X-Ray 加密資源、稽核 X-Ray 組態歷程記錄，以及根據資源變更傳送通知。如需詳細資訊，請參閱AWS X-Ray 開發人員指南 AWS Config中的追蹤 X-Ray 加密組態變更。

## AWS Service Management Connector

用 AWS Service Management Connector 於 ServiceNow 可以使用彙總 AWS Config 器同步處理來自多個帳戶和區域的資料。如需詳細資訊，請參閱《AWS Service Management Connector 管理員指南》AWS Config ServiceNow中的〈整合〉。

## Amazon API Gateway

您可以用 AWS Config 來記錄對 API Gateway API 資源所做的組態變更，並根據資源變更傳送通知。保留 API Gateway 資源的組態變更歷史記錄很實用，可用於解決操作問題、稽核和合規使用案例。如需詳細資訊，請參閱《API Gateway 開發人員指南》 AWS Config中的使用監控 API Gateway API 組態。

# 補充資料及相關資源

以下相關資源可協助您使用此服務。

- AWS Config— 主要網頁以取得相關資訊 AWS Config。
- AWS Config 定價
- 技術常見問答集
- AWS Config 規則開發套件 (RDK) — 一種開放原始碼工具，可協助您設定 AWS Config、撰寫規則，然後使用各種 AWS 資源類型進行測試。
- 合作夥伴 — 完全整合的合作夥伴產品連結，可協助您視覺化、監控及管理組態串流、組態快照或組態歷程記錄中的資料。 AWS Config

- 課程和工作坊 — 除了可以幫助提高 AWS 技能並獲得實踐經驗的自定進度實驗室之外，還可以鏈接到基於角色和專業課程的鏈接。
- AWS 開發人員中心 — 探索教學課程、下載工具，以及瞭解 AWS 開發人員活動。
- AWS 開發人員工具 — 開發人員工具、SDK、IDE 工具組，以及用於開發和管理 AWS 應用程式的命令列工具的連結。
- 入門資源中心 — 瞭解如何設定 AWS 帳戶、加入 AWS 社群，以及啟動您的第一個應用程式。
- 實作教學課程 — 按照 step-by-step 教學課程啟動您的第一個應用程式 AWS。
- AWS 白皮書 — 完整的技術 AWS 白皮書清單連結，涵蓋架構、安全性和經濟等主題，並由 AWS 解決方案架構師或其他技術專家撰寫。
- AWS Support 中心 — 建立和管理 AWS Support 案例的中心。同時也包含其他實用資源的連結，例如論壇、技術常見問答集、服務健康狀態和 AWS Trusted Advisor.
- AWS Support— 有關資訊的主要網頁 AWS Support one-on-one, 快速回應的支援管道，可協助您在雲端中建置和執行應用程式.
- 聯絡我們 – 查詢有關 AWS 帳單、帳戶、事件、濫用與其他問題的聯絡中心。
- AWS 網站條款 — 有關我們的版權和商標的詳細資訊；您的帳戶、授權和網站存取權限；以及其他主題。

## AWS 軟體開發套件 AWS Config

AWS 軟體開發套件 (SDK) 可讓您更輕鬆地建置存取具成本效益、可擴充且可靠的 AWS 基礎架構服務的應用程式。透過 AWS 開發套件，您可以在幾分鐘內開始使用可下載的單一套件，其中包括程式庫、程式碼範例和參考文件。下表列出可用於以程式設計方式存取的可用 SDK 和協力廠商 AWS Config 程式庫。

| 存取類型 | 描述 |
| --- | --- |
| AWS 開發套件 | AWS 提供下列軟體開發套件：<br>• AWS 適用於 C++ 文件的 SDK<br>• AWS Mobile SDK for iOS 文件<br>• 適用於 Go 的AWS 開發套件文件<br>• AWS SDK for Java 文件<br>• AWS 適用於 JavaScript 文件的 SDK<br>• AWS SDK for .NET 文件 |

| 存取類型 | 描述 |
| --- | --- |
| | • AWS SDK for PHP 文件<br>• AWS SDK for Python (Boto) 文件<br>• AWS SDK for Ruby 文件 |
| 第三方程式庫 | 開發 AWS 人員社群中的開發人員也會提供自己的程式庫，您可以在下列 AWS 開發人員中心找到這些資料庫：<br>• AWS Java 開發人員中心<br>• AWS JavaScript 開發人員中心<br>• AWS PHP 開發人員中心<br>• AWS Python 開發人員中心<br>• AWS Ruby 開發人員中心<br>• AWS 開發人員中心 |

# 開始使用 AWS Config

AWS Config 提供您中 AWS 資源組態的詳細檢視 AWS 帳戶。使用 AWS Config，您可以檢閱組態中的變更以及 AWS 資源之間的關係、探索資源組態歷程記錄，以及使用規則來判斷符合性。如需詳細資訊，請參閱什麼是 AWS Config？ 以及如何 AWS Config 工作。

## 註冊成為 AWS

主題

- 註冊一個 AWS 帳戶
- 建立具有管理權限的使用者

### 註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

### 建立具有管理權限的使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

# 開始使用的方法 AWS Config

註冊之後 AWS 帳戶，您可以開 AWS Config 始使用 AWS Management Console、 AWS CLI 或 AWS SDK。

- 使用主控 AWS Config 台進行設定
- AWS Config 使用設定 AWS CLI
- 搭配 AWS SDK 使用 AWS Config 服務

# 使用主控 AWS Config 台進行設定

提 AWS Management Console 供快速且簡化的設定程序 AWS Config。

## 設定

使用主控台 AWS Config 進行設定

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 如果這是您第一次開啟 AWS Config 主控台，或是在新區域 AWS Config 中進行設定， AWS Config 主控台頁面如下所示：

3. 選擇一鍵式設置以 AWS Config 根據 AWS 最佳實踐啟動。您也可以選擇 開始 執行更詳細的設定流程。

主題

- 一鍵式設定
- 手動設定

## 一鍵式設定

AWS Config 一鍵式設定可減少手動選擇的次數，協助簡化 AWS Config 主控台客戶的入門程序。若要完成所有手動選取的設定程序，請參閱手動設定。

使用一鍵式設定使 AWS Config 用主控台進行設定

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 選擇 一鍵式設定。

設定 頁面包含三個步驟，但透過 一鍵式設定 工作流程會自動導向到步驟 3 (檢閱)。以下提供該程序的細節。

- 設定：選取 AWS Config 主控台記錄資源和角色的方式，並選擇傳送組態歷史記錄和組態快照檔案的位置。
- 規則：對於支援規則的區域，此子區段可供您設定可新增至帳戶的初始 AWS 受管規則。

  設定完成後， AWS Config 將根據您選擇的規則評估您的 AWS 資源。您可以建立其他規則，以及在設定後更新帳戶中的現有規則。如需有關規則的詳細資訊，請參閱管理 AWS Config 規則。
- 檢閱：驗證您的設定詳細資料。

### 設定

#### 記錄策略

已為您選取記錄具有可自訂覆寫項的所有資源類型的選項。 AWS Config 會記錄此區域中所有目前及 future 支援的資源類型。如需詳細資訊，請參閱《支援的資源類型》。

- 預設設定

  默認記錄頻率為您設置為連續。這表示每當發生變更時，都會持續 AWS Config 記錄組態變更。

AWS Config 還支持將錄製頻率設置為每日的選項。如果您在安裝後選取此選項，您將會收到一個組態項目 (CI)，代表過去 24 小時期間內資源的最新狀態，前提是它與先前的 CI 記錄不同時。如需詳細資訊，請參閱記錄頻率。

> **Note**
>
> AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

- 覆寫設定 — 選擇性

  選擇性地在設定之後，您可以覆寫特定資源型態的記錄頻率，或從記錄中排除特定資源型態。若要覆寫預設設定，請選擇 AWS Config 主控台左側導覽中的 [設定]，然後選擇 [編輯]。

記錄資源時的考量

大量的 AWS Config 評估

與之後的月份相比，您可能會注意到在使用 AWS Config 錄製首個月期間帳戶中的活動有所增加。在初始啟動安裝程序期間， AWS Config 會對 AWS Config 您帳戶中選取要記錄的所有資源執行評估。

如果您正在執行暫時工作負載，可能會看到來自 AWS Config 的活動增加，因其會記錄與建立和刪除這些暫時資源相關聯的組態變更。暫時性工作負載是暫時使用因需要而載入和執行的運算資源。範例包括 Amazon Elastic Compute Cloud (Amazon EC2) Spot 執行個體、Amazon EMR 作業和 AWS Auto Scaling。如果您想要避免因執行臨時工作負載而增加的活動，您可以設定組態錄製程式以將這些資源類型排除在記錄之外，或在關 AWS Config 閉的情況下在單獨的帳戶中執行這些類型的工作負載，以避免增加組態記錄和規則評估。

全域資源類型 | Aurora 全域叢集最初包含在記錄中

資`AWS::RDS::GlobalCluster`源類型將記錄在啟用配置記錄器的所有支援 AWS Config 區域中。

如果您不希望在所有已啟用的區域中記錄 `AWS::RDS::GlobalCluster`，您可以在設定後從記錄中排除此資源類型。在左側導覽列中，選擇設定，然後選擇基本。從編輯移至記錄方法區段的覆蓋設定，選擇 `AWS::RDS::GlobalCluster`，並選擇覆寫「從記錄中排除」。

全域資源類型 | IAM 資源類型最初會從記錄中排除

「所有全域記錄的 IAM 資源類型」最初會從記錄中排除，以協助您降低成本。此配套包含 IAM 使用者、群組、角色和客戶管理政策。選擇移除以移除覆寫，並將這些資源包含在您的記錄中。

此附註不涵蓋美國東部 (維吉尼亞北部)。全域 IAM 資源類型最初包含在美國東部 (維吉尼亞北部) 區域，因為該區域充當全球 IAM 資源類型的主區域。

此外，在 2022 年 2 月 AWS Config 之後支援的區域中 `AWS::IAM::User` `AWS::IAM::Group``AWS::IAM::Role`，無法記錄全域 IAM 資源類型 (、、和`AWS::IAM::Policy`)。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

資料控管

在本節中為您選擇了 AWS Config 保留 7 年（2557 天）的默認數據保留期。

系統會為您選取「使用現有的 AWS Config 服務連結角色」選項，並將其設定為AWS Config 角色。服務連結角色由預先定義， AWS Config 並包含服務呼叫其他 AWS 服務所需的所有權限。

交付方法

在這個區段為您選取從您的帳戶選擇儲存貯體選項。此選項將預設為您帳戶中以格式命名的值區`config-bucket-`*`accountid`*。例如 `config-bucket-012345678901`。如果沒有以此格式建立的儲存貯體，系統會為您建立一個。若要建立儲存貯體，請參閱 Amazon Simple Storage Service 使用者指南中的建立儲存貯體。

如需有關 S3 儲存貯體的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》的《儲存貯體概觀》。

### 規則

這個步驟不會為您選取 AWS 受管規則 下的任何規則。反之，我們建議您在設定完帳戶後建立與更新規則。

### 檢閱

檢閱您的 AWS Config 設定詳細資料。您可以返回編輯每個區段的變更。選擇「確認」以完成設定 AWS Config。

## 手動設定

透過 [開始使用] 工作流程，您可以執行所有手動選取的設定程序，以開始使用主 AWS Config 控台。如需簡化的入門程序，請參閱一鍵式設定。

AWS Config 使用主控台進行設定開始使用

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。

2. 選擇開始使用。

設定頁面包含三個步驟。以下提供在您選擇 開始 之後，該程序的細節。

- 設定：選取 AWS Config 主控台記錄資源和角色的方式，並選擇傳送組態歷史記錄和組態快照檔案的位置。
- 規則：對於支援規則的區域，此子區段可供您設定可新增至帳戶的初始 AWS 受管規則。

  設定完成後， AWS Config 將根據您選擇的規則評估您的 AWS 資源。您可以建立其他規則，以及在設定後更新帳戶中的現有規則。如需有關規則的詳細資訊，請參閱管理 AWS Config 規則。
- 檢閱：驗證您的設定詳細資料。

## 設定

### 記錄策略

在記錄方法區段中，選擇記錄策略。您可以指定要 AWS Config 記錄的 AWS 資源。

All resource types with customizable overrides

設定 AWS Config 以記錄此區域中所有目前與 future 支援之資源型態的組態變更。您可以覆寫特定資源類型的記錄頻率，或從記錄中排除特定資源類型。如需詳細資訊，請參閱《支援的資源類型》。

- 預設設定

  為所有目前和未來支援的資源類型設定預設記錄頻率。如需詳細資訊，請參閱記錄頻率。
  - 連續錄製 — 每當發生變更時，都 AWS Config 會持續記錄組態變更。
  - 每日記錄 – 您可接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。

  > **Note**
  > AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

- 覆寫設定

覆寫特定資源類型的記錄頻率，或從記錄中排除特定資源類型。如果您變更某資源類型的記錄頻率，則已記錄的組態項目會保持不變。

Specific resource types

設 AWS Config 定為僅記錄您指定之資源類型的組態變更。

- 特定資源類型

  選擇要記錄的資源類型及其頻率。如需詳細資訊，請參閱記錄頻率。

  - 連續錄製 — 每當發生變更時，都 AWS Config 會持續記錄組態變更。
  - 每日記錄 – 您可接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。

  > **Note**
  > AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

  如果您變更某資源類型的記錄頻率，則已記錄的組態項目會保持不變。

記錄資源時的考量

大量的 AWS Config 評估

與之後的月份相比，您可能會注意到在使用 AWS Config 錄製首個月期間帳戶中的活動有所增加。在初始啟動安裝程序期間， AWS Config 會對 AWS Config 您帳戶中選取要記錄的所有資源執行評估。

如果您正在執行暫時工作負載，可能會看到來自 AWS Config 的活動增加，因其會記錄與建立和刪除這些暫時資源相關聯的組態變更。暫時性工作負載是暫時使用因需要而載入和執行的運算資源。範例包括 Amazon 彈性運算雲端 (Amazon EC2) 競價型執行個體、亞馬遜 EMR 任務和 AWS Auto Scaling. 如果您想要避免因執行臨時工作負載而增加的活動，您可以設定組態錄製程式以將這些資源類型排除在記錄之外，或在關 AWS Config 閉的情況下在單獨的帳戶中執行這些類型的工作負載，以避免增加組態記錄和規則評估。

Considerations: All resource types with customizable overrides

全域記錄的資源類型 | Aurora 全域叢集最初包含在記錄中

資`AWS::RDS::GlobalCluster`源類型將記錄在啟用配置記錄器的所有支援 AWS Config 區域中。

如果您不想在所有已啟用的區域中記錄 `AWS::RDS::GlobalCluster`，請選擇「AWS RDS GlobalCluster」，然後選擇覆寫「從記錄中排除」。

全域資源類型 | IAM 資源類型最初會從記錄中排除

一開始會從記錄中排除全域 IAM 資源類型，以協助您降低成本。此配套包含 IAM 使用者、群組、角色和客戶管理政策。選擇移除以移除覆寫，並將這些資源包含在您的記錄中。

美國東部 (維吉尼亞北部) 例外。全域 IAM 資源類型最初包含在美國東部 (維吉尼亞北部) 區域，因為該區域充當全球 IAM 資源類型的主區域。

此外，在 2022 年 2 月 AWS Config 之後支援的區域中 `AWS::IAM::User` `AWS::IAM::Group``AWS::IAM::Role`，無法記錄全域 IAM 資源類型 (、、和`AWS::IAM::Policy`)。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

限制

您最多可以增加到 100 個頻率覆寫及 600 個排除覆寫。

下列資源類型不支援每日記錄：

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

區域可用性

在指定 AWS Config 要追蹤的資源型態之前，請先勾選「依可用區域的資源涵蓋範圍」，以查看您設定的「 AWS 區域」中是否支援資源型態 AWS Config。如果至少一個「區域」支援某個資源類型，則您可以 AWS Config 在所支援的所有「區域」中啟用該資源類型的記錄 AWS Config，即使您設定的「 AWS 區域」不支援指定的資源類型也一樣 AWS Config。

限制

如果所有資源類型具有相同頻率，則無限制。如果至少有一種資源類型設定為「持續」，您最多可以使用「每日」頻率增加 100 個資源類型。

以下資源類型不支援每日頻率：

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

資料控管

- 對於資料保留期，請選擇預設保留期限以保留 AWS Config 資料 7 年 (2557)，或為記錄的項目設定自訂保留期。 AWS Config

  AWS Config 允許您通過指定的保留期限來刪除您的數據`ConfigurationItems`。當您指定保留期間時， AWS Config 會在指定`ConfigurationItems`的期間內保留您的。您可以選擇最少 30 天至最多 7 年（2557 天）之間的期限。 AWS Config 刪除超過指定保留期限的資料。
- 對於的 IAM 角色 AWS Config，請從您的帳戶中選擇現有的 AWS Config 服務連結角色或 IAM 角色。
  - 服務連結角色由預先定義， AWS Config 並包含服務呼叫其他 AWS 服務所需的所有權限。

    > **Note**
    >
    > 建議：使用服務連結角色
    > 建議您使用服務連結角色。服務連結角色會新增所有必要的權限， AWS Config 以便如預期般執行。

  - 否則，請從其中一個預先存在的角色和權限政策中選擇 IAM 角色。

    > **Note**
    >
    > AWS Organizations 可以防止存取的授權原則
    > 如果您使用預先存在的 IAM 角色，請確保沒有授權政策阻 AWS Config 止您記錄資源的權限。 AWS Organizations 如需有關的授權原則的詳細資訊 AWS Organizations，請參閱《AWS Organizations 使用指南》AWS Organizations中的〈管理策略〉。
    > 重複使用 IAM 角色時保持最低權限
    > 如果您使用的 AWS 服務使用 AWS Config，例如 AWS Security Hub 或 AWS Control Tower，且已建立 IAM 角色，請確保您在設定時使用的 IAM 角色保 AWS Config 持與預先

存在的 IAM 角色相同的最低許可。您必須這麼做，以確保其他 AWS 服務能如預期般繼續執行。
例如，如果 AWS Control Tower 具有允許 AWS Config 讀取 S3 物件的 IAM 角色，請確保將相同的許可授與您在設定時使用的 IAM 角色 AWS Config。否則，它可能會干擾 AWS Control Tower 操作方式。

交付方法

- 請為 交付方法 選擇 AWS Config 傳送組態歷史記錄和組態快照檔案的目標 S3 儲存貯體：
  - 建立儲存貯體：在 S3 儲存貯體名稱 中輸入您的 S3 儲存貯體名稱。

    您輸入的名稱在 Amazon S3 所有的現有儲存貯體名稱中必須是唯一的。其中一種協助確保唯一性的方法是在儲存貯體名稱的前面加上前綴。例如：您組織的名稱。您無法在建立之後變更儲存貯體的名稱。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的儲存貯體限制。
  - 選擇您帳戶的儲存貯體：在 S3 儲存貯體名稱 中選擇您慣用的儲存貯體。
  - 從其他帳戶選擇儲存貯體：在 S3 儲存貯體名稱 中輸入儲存貯體名稱。

    > **Note**
    >
    > 值區權限
    > 如果您從其他帳戶選擇值區，則該值區必須具有可授與存取權限的政策 AWS Config。如需詳細資訊，請參閱 適用於 AWS Config 交付通道的 Amazon S3 儲存貯體的許可。

- 對於 Amazon SNS 主題，請選擇傳送 Amazon SNS 主題的串流組態變更和通知，以 AWS Config 傳送組態歷史記錄交付、組態快照交付和合規等通知。
- 如果您選擇將 AWS Config 串流傳送至 Amazon SNS 主題，請選擇目標主題：
  - 建立主題：在 主題名稱 中輸入 SNS 主題的名稱。
  - 選擇您帳戶中的主題：為 主題名稱 選取您偏好的主題。
  - 從其他帳戶選擇主題：在 主題 ARN 中輸入主題的 Amazon Resource Name (ARN)。如果您從其他帳戶選擇主題，則該主題必須具有可授與存取權限的策略 AWS Config。如需詳細資訊，請參閱 Amazon SNS 主題的許可。

    > **Note**
    >
    > Amazon SNS 主題的區域

Amazon SNS 主題必須與您設定的區域位於相同的區域中 AWS Config。

### 規則

如果您要在支援規則的「地區」 AWS Config 中進行設定，請選擇「下一步」。如需詳細資訊，請參閱新增、更新及刪除 AWS Config 規則。

否則，請選擇 確認。

### 檢閱

檢閱您的 AWS Config 設定詳細資料。您可以返回編輯每個區段的變更。選擇「確認」以完成設定 AWS Config。

### 如需詳細資訊

如需查詢您帳戶中現有資源及了解您資源組態的資訊，請參閱檢視 資源組態和歷史記錄。

您也可以使用 Amazon 簡單佇列服務以程式設計方式監控 AWS 資源。如需詳細資訊，請參閱 使用 Amazon SQS 監控 AWS 資源變更。

## AWS Config 使用設定 AWS CLI

AWS CLI 這是一個統一的工具來管理您的 AWS 服務。只要下載和設定一個工具，您就可以從命令列控制多個 AWS 服務，並使用指令碼將它們自動化。若要取得有關 AWS CLI 和安裝 AWS CLI 工具的更多資訊，請參閱《AWS Command Line Interface 使用指南》中的以下內容。

- AWS Command Line Interface 使用者指南
- 設定 AWS Command Line Interface

如有必要，請輸入`aws configure`以配置 AWS CLI 以使用可用的 AWS Config 「 AWS 區域」。

### 設定

請參閱下列主題以進行 AWS Config 設定 AWS CLI。

主題

- 必要條件
- 從 AWS Config 開始 AWS CLI

- 驗證 AWS Config 是否已成功啟動 AWS CLI

## 必要條件

在設 AWS 定之前 AWS CLI，您需要建立 Amazon S3 儲存貯體、Amazon SNS 主題以及具有附加政策的 IAM 角色做為先決條件。然後，您可以使用 AWS CLI 來指定的值區、主題和角色 AWS Config。請遵循此程序設定 AWS Config的先決條件。

內容

- 建立 Amazon S3 儲存貯體
- 建立 Amazon SNS 主題
- 建立 IAM 角色

### 建立 Amazon S3 儲存貯體

如果帳戶中已有想要使用的 Amazon S3 儲存貯體，請跳過此步驟，前往《建立 Amazon SNS 主題》。

使用 S3 主控台

建立儲存貯體

1. 前往 https://console.aws.amazon.com/s3/ 開啟 Amazon S3 主控台。
2. 選擇建立儲存貯體。
3. 在 Bucket name (儲存貯體名稱) 中，為儲存貯體輸入符合 DNS 規範的名稱。

   儲存貯體名稱必須；

   - 在所有 Amazon S3 中都為唯一。
   - 長度必須介於 3 與 63 個字元之間。
   - 不含大寫字元。
   - 以小寫字母或數字開頭。

   建立儲存貯體後，便無法變更其名稱。確認您選擇的儲存貯體名稱在 Amazon S3 所有的現有儲存貯體名稱中是唯一的。如需儲存貯體命名規則和慣例的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的《儲存貯體法規與限制》。

> **Important**
>
> 避免在值區名稱中包含敏感資訊。在指向儲存貯體中之物件的 URL 中，會顯示儲存貯體名稱。

4. 在「地區」中，選擇您要儲存貯體所在的「 AWS 區域」。

   建議您選擇接近您的區域以充分降低延遲及成本，並因應法規要求。除非您明確地將存放在區域中的物件傳輸到其他區域，否則物件絕對不會離開該區域。如需 Amazon S3 AWS 區域的清單，請參閱AWS Amazon Web Services 一般參考.

5. 在 Bucket settings for Block Public Access (封鎖公開存取的儲存貯體設定) 中，選擇要套用至儲存貯體的封鎖公開存取設定。

   除非您知道您需要針對使用案例關閉一或多個設定，例如託管公有網站，否則建議您將所有設定保持啟用狀態。另外針對您在儲存貯體上建立的所有存取點，也會啟用封鎖公開存取設定。如需有關封鎖公開存取的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的《使用 Amazon S3 封鎖公開存取》。

6. (選用) 如果您要啟用 S3 物件鎖定：

   a. 選擇 Advanced settings (進階設定)，然後閱讀出現的訊息。

   > **Important**
   >
   > 您只能在建立儲存貯體時啟用 S3 物件鎖定。如果您啟用儲存貯體的物件鎖定，稍後無法加以停用。啟用物件鎖定也會啟用儲存貯體的版本控制。啟用儲存貯體的物件鎖定後，您必須先設定物件鎖定設定，之後才能保護儲存貯體中的任何物件。如需設定物件防護的詳細資訊，請參閱《使用 Amazon S3 主控台設定 S3 物件鎖定》。

   b. 如果要啟用物件鎖定，請在文字方塊中輸入啟用，然後選擇確認。

   如需 S3 物件鎖定功能的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的《使用 Amazon S3 物件鎖定功能鎖定物件》。

7. 選擇建立儲存貯體。

使用 AWS 軟體開發套件

使用 AWS SDK 建立值區時，必須建立用戶端，然後使用用戶端傳送要求以建立值區。最佳實務是，您應該在同一個 AWS 區域中建立用戶端和儲存貯體。如果您在建立用戶端或儲存貯體時未指定區域，則 Amazon S3 會使用預設的美國東部 (維吉尼亞北部) 區域。

若要建立用戶端以存取雙堆疊端點，您必須指定 AWS 區域. 如需詳細資訊，請參閱《Amazon S3 雙堆疊端點》。如需可用的清單 AWS 區域，請參閱中的區域和端點AWS 一般參考。

建立用戶端時，區域會對應至區域特定的端點。用戶端會使用此端點來與 Amazon S3：`s3.<region>.amazonaws.com` 通訊。如果您的區域在 2019 年 3 月 20 日之後啟動，您的用戶端和儲存貯體必須位於相同區域中。不過，您可以在美國東部 (維吉尼亞北部) 區域中使用用戶端，以便在 2019 年 3 月 20 日之前推出的任何區域中建立儲存貯體。如需詳細資訊，請參閱《舊版端點》。

這些 AWS SDK 程式碼範例會執行下列工作：

- 透過明確指定 AWS 區域 來建立用戶端 – 在此範例中，用戶端使用 `s3.us-west-2.amazonaws.com` 端點與 Amazon S3 通訊。您可指定任何 AWS 區域。如需的清單 AWS 區域，請參閱AWS 一般參考中的區域和端點。
- 透過僅指定儲存貯體名稱來傳送建立儲存貯體 要求 — 用戶端會向 Amazon S3 傳送要求，以在您建立用戶端的區域中建立儲存貯體。
- 擷取儲存貯體位置的相關資訊 — Amazon S3 會將儲存貯體位置資訊存放在與儲存貯體相關聯的 location 子資源中。

下列程式碼範例會示範如何使用`CreateBucket`。

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
        /// <summary>
```

```
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

建立啟用物件鎖定的值區。

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
```

```
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考CreateBucket中的。

## Bash

### AWS CLI 使用 Bash 腳本

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
```

```
  fi
}

##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }
```

```
  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
```

```
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考CreateBucket中的。

## C++

### 適用於 C++ 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
bool AwsDoc::S3::CreateBucket(const Aws::String &bucketName,
                              const Aws::Client::ClientConfiguration
 &clientConfig) {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    //TODO(user): Change the bucket location constraint enum to your target
 Region.
    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
```

```
        auto err = outcome.GetError();
        std::cerr << "Error: CreateBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    }
    else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for C++ API 參考CreateBucket中的。

## CLI

### AWS CLI

範例 1：若要建立值區

下列`create-bucket`範例會建立名為的值區`my-bucket`：

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1
```

輸出：

```
{
    "Location": "/my-bucket"
}
```

如需詳細資訊，請參閱 Amazon S3 使用者指南中的建立儲存貯體。

範例 2：若要建立強制擁有者的值區

下列`create-bucket`範例會建立名`my-bucket`為使用 S3 物件擁有權強制執行儲存貯體擁有者設定的儲存貯體。

```
aws s3api create-bucket \
```

```
    --bucket my-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

輸出：

```
{
    "Location": "/my-bucket"
}
```

如需詳細資訊，請參閱《Amazon S3 使用者指南》中的控制物件的所有權並停用 ACL。

範例 3：在「us-east-1」區域之外建立值區

下列`create-bucket`範例會建立區域`my-bucket`中名為的值`eu-west-1`區。位於以外的區域`us-east-1`需要指定適當`LocationConstraint`的區域，才能在所需的區域中建立值區。

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

輸出：

```
{
    "Location": "http://my-bucket.s3.amazonaws.com/"
}
```

如需詳細資訊，請參閱 Amazon S3 使用者指南中的建立儲存貯體。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考CreateBucket中的。

## Go

### SDK for Go V2

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(name string, region string) error {
 _, err := basics.S3Client.CreateBucket(context.TODO(), &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  log.Printf("Couldn't create bucket %v in Region %v. Here's why: %v\n",
   name, region, err)
 }
 return err
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Go API 參考CreateBucket中的。

## Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

建立儲存貯體。

```
import software.amazon.awssdk.core.waiters.WaiterResponse;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketResponse;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.s3.waiters.S3Waiter;
import java.net.URISyntaxException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateBucket {
    public static void main(String[] args) throws URISyntaxException {
        final String usage = """

                Usage:
                    <bucketName>\s

                Where:
                    bucketName - The name of the bucket to create. The bucket
 name must be unique, or an error occurs.
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String bucketName = args[0];
        System.out.format("Creating a bucket named %s\n", bucketName);
        Region region = Region.US_EAST_1;
        S3Client s3 = S3Client.builder()
                .region(region)
```

```
                .build();

        createBucket(s3, bucketName);
        s3.close();
    }

    public static void createBucket(S3Client s3Client, String bucketName) {
        try {
            S3Waiter s3Waiter = s3Client.waiter();
            CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            s3Client.createBucket(bucketRequest);
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            // Wait until the bucket is created and print out the response.
            WaiterResponse<HeadBucketResponse> waiterResponse =
 s3Waiter.waitUntilBucketExists(bucketRequestWait);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println(bucketName + " is ready");

        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

建立啟用物件鎖定的值區。

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
 bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();
```

```
        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考CreateBucket中的。

## JavaScript

### 適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

建立儲存貯體。

```
import { CreateBucketCommand, S3Client } from "@aws-sdk/client-s3";

const client = new S3Client({});

export const main = async () => {
  const command = new CreateBucketCommand({
    // The name of the bucket. Bucket names are unique and have several other
 constraints.
    // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
    Bucket: "bucket-name",
  });

  try {
    const { Location } = await client.send(command);
    console.log(`Bucket created with location ${Location}`);
  } catch (err) {
```

```
    console.error(err);
  }
};
```

- 如需詳細資訊，請參閱《AWS SDK for JavaScript 開發人員指南》。
- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考CreateBucket中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK CreateBucket中的 Kotlin API 參考。

## PHP

### 適用於 PHP 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

建立儲存貯體。

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
$exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for PHP API 參考CreateBucket中的。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

使用預設設定建立儲存貯體。

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

透過生命週期組態建立版本控制儲存貯體。

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
```

```
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件CreateBucket中的 Python (博托 3) API 參考。

## Ruby

### 適用於 Ruby 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
require "aws-sdk-s3"

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      "None. You must create a bucket before you can get its location!"
    else
```

```
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("doc-example-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Ruby API 參考CreateBucket中的。

## Rust

### 適用於 Rust 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
pub async fn create_bucket(
    client: &Client,
    bucket_name: &str,
    region: &str,
) -> Result<CreateBucketOutput, SdkError<CreateBucketError>> {
    let constraint = BucketLocationConstraint::from(region);
    let cfg = CreateBucketConfiguration::builder()
        .location_constraint(constraint)
```

```
        .build();
    client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await
}
```

- 如需 API 的詳細資訊，請參閱 AWS SDK CreateBucket中的 Rust API 參考資料。

## SAP ABAP

### 適用於 SAP ABAP 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    TRY.
        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
        ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- 如需 API 詳細資訊，請參閱 AWS SDK CreateBucket中的 SAP ABAP API 參考資料。

Swift

適用於 Swift 的 SDK

> **Note**
>
> 這是適用於預覽版本 SDK 的發行前版本文件。內容可能變動。

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
public func createBucket(name: String) async throws {
    let config = S3ClientTypes.CreateBucketConfiguration(
        locationConstraint: .usEast2
    )
    let input = CreateBucketInput(
        bucket: name,
        createBucketConfiguration: config
    )
    _ = try await client.createBucket(input: input)
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK CreateBucket中的斯威夫特 API 參考。

> **Note**
>
> 您也可以使用其他帳戶的 Amazon S3 儲存貯體，但您可能需要建立適用於該儲存貯體的政策，將存取許可授予 AWS Config。如需授予 Amazon S3 儲存貯體許可的相關資訊，請參閱《適用於 AWS Config 交付通道的 Amazon S3 儲存貯體的許可》，然後前往《建立 Amazon SNS 主題》。

## 建立 Amazon SNS 主題

如果帳戶中已有想要使用的 Amazon SNS 主題，請跳過此步驟，前往《建立 IAM 角色》。

使用 SNS 主控台

建立 Amazon SNS 主題

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 執行以下任意一項：
   - 如果您 AWS 帳戶 之前沒有建立任何主題，請閱讀首頁上 Amazon SNS 的說明。
   - 如果主題已在您 AWS 帳戶 之前的下方建立，請在導覽面板上選擇「主題」。
3. 在主題頁面上，選擇建立主題。
4. 在 Create topic (建立主題) 頁面上，於 Details (詳細資訊) 區段中，執行以下作業：
   a. 對於 Type (類型)，選擇主題類型 (Standard (標準)或FIFO。
   b. 輸入新主題的名稱。對於FIFO 主題，新增.fifo到名稱的結尾。
   c. (選用) 為主題輸入 Display name (顯示名稱)。
   d. (選用) 對於 FIFO 主題，您可以選擇內容型訊息重複資料刪除功能，以啟用預設的重複訊息刪除功能。如需詳細資訊，請參閱《刪除重複 FIFO 主題的郵件》。
5. (選用) 展開 Encryption (加密) 區段並執行下列動作。如需詳細資訊，請參閱靜態加密。
   a. 選擇 Enable encryption (啟用加密)。
   b. 指定客戶主金鑰 (CMK)。如需詳細資訊，請參閱重要用語。

      每個 CMK 類型均會顯示 Description (描述)、Account (帳戶) 和 CMK ARN。

> **Important**
>
> 若您並非 CMK 的擁有者，或者您登入的帳戶並無 `kms:ListAliases` 和 `kms:DescribeKey` 的許可，即無法在 Amazon SNS 主控台上檢視 CMK 相關資訊。
> 請要求 CMK 的所有人提供許可。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的AWS KMS API 許可：動作和資源參考。

- 預設會選取適用於 Amazon SNS 的 AWS 受管 CMK (預設) 別名/AWS/SNS。

> **Note**
>
> 請謹記以下幾點：
>
> - 第一次使用指定主題適 AWS Management Console 用於 Amazon SNS 的 AWS 受管 CMK 時， AWS KMS 會建立適用於 Amazon SNS 的 AWS 受管 CMK。
> - 或者，當您第一次對已啟用 SSE 的主題使用`Publish`動作時， AWS KMS 會為 Amazon SNS 建立 AWS 受管 CMK。

- 若要使用您的自訂 CMK AWS 帳戶，請選擇 [客戶主金鑰 (CMK)] 欄位，然後從清單中選擇自訂 CMK。

> **Note**
>
> 如需建立自訂 CMK 的說明，請參閱 AWS Key Management Service 開發人員指南中的建立金鑰

- 若要使用您 AWS 帳戶 或其他 AWS 帳戶的自訂 CMK ARN，請在「客戶主金鑰 (CMK)」欄位中輸入該自訂 CMK ARN。

6. (選用) 根據預設，只有主題擁有者可以發布或訂閱主題。若要設定其他存取許可，請展開 Access policy (存取政策) 區段。如需詳細資訊，請參閱《Amazon SNS 中的身分識別和存取管理》和《Amazon SNS 存取控制範例案例》。

> **Note**
>
> 當您使用主控台建立主題時，預設政策會使用 `aws:SourceOwner` 條件金鑰。此金鑰類似於 `aws:SourceAccount`。

7. (選用) 若要設定 Amazon SNS 如何在訊息傳遞嘗試失敗後重試，請展開 Delivery retry policy (HTTP/S) (傳遞重試政策 (HTTP/S)) 區段。如需詳細資訊，請參閱《Amazon SNS 訊息傳遞重試》。
8. (選擇性) 若要設定 Amazon SNS 記錄訊息交付的方式 CloudWatch，請展開交付狀態記錄區段。如需詳細資訊，請參閱 Amazon SNS 訊息傳遞狀態。
9. (選用) 若要將中繼資料標籤新增至主題，請展開 Tags (標籤) 區段，輸入 Key(金鑰) 和 Value (值) (選用)，然後選擇 Add tag (新增標籤)。如需詳細資訊，請參閱《標記 Amazon SNS 主題》。

10. 請選擇建立主題。

    隨即建立主題並顯示***MyTopic***頁面。

    主題的 Name (名稱)、ARN、選用的 Display name (顯示名稱) 以及 Topic owner (主題擁有者) 的 AWS 帳戶 ID 會顯示在 Details (詳細資訊) 區段中。

11. 將主題 ARN 複製到剪貼簿，例如：

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

訂閱 Amazon SNS 主題的電子郵件地址

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在左導覽窗格中，選擇訂閱。
3. 在訂閱頁面，選擇建立訂閱。
4. 在建立訂閱頁面上，於詳細資訊區段中，執行以下作業：

   a. 對於ARN 主題，選擇主題的 Amazon 資源名稱 (ARN)。

   b. 在 Protocol (通訊協定)，選擇端點類型。可用的端點類型為：

      - HTTP/HTTPS
      - Email/Email-JSON (電子郵件/電子郵件-JSON)
      - Amazon 數據 Firehose
      - Amazon SQS

        > **Note**
        > 若要訂閱SNS FIFO 主題，請選擇此選項。

      - AWS Lambda
      - 平台應用程式端點
      - SMS

   c. 對於Endpoint (端點)，輸入端點值，例如電子郵件地址或 Amazon SQS 佇列的 ARN。

   d. 僅限 Firehose 端點：對於訂閱角色 ARN，請指定您為寫入 Firehose 交付串流而建立的 IAM 角色的 ARN。如需詳細資訊，請參閱訂閱 Amazon SNS 的 Firehose 交付串流的先決條件主題。

e. (選擇性) 對於 Firehose、Amazon SQS、HTTP/S 端點，您也可以啟用原始訊息傳遞。如需詳細資訊，請參閱《Amazon SNS 原始訊息交付》。

f. (選用) 若要設定篩選政策，請展開 Subscription filter policy (訂閱篩選政策) 區段。如需詳細資訊，請參閱《Amazon SNS 訂閱篩選政策》。

g. (選用) 若要設定訂閱的無效字母佇列，請展開 Redrive policy (dead-letter queue) (重新磁碟機政策 (無效字母佇列)) 區段。如需詳細資訊，請參閱《Amazon SNS 無效字母佇列 (DLQ)》。

h. 選擇建立訂閱。

   主控台會建立訂閱並開啟訂閱的 Details (詳細資訊) 頁面

## 使用 AWS 軟體開發套件

要使用 AWS SDK，您必須使用憑據對其進行配置。如需詳細資訊，請參閱 AWS SDK和工具參考指南中的共享的配置和認證文件。

下列程式碼範例會示範如何使用`CreateTopic`。

### .NET

#### AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

建立具有特定名稱的主題。

```
using System;
using System.Threading.Tasks;
using Amazon.SimpleNotificationService;
using Amazon.SimpleNotificationService.Model;

/// <summary>
/// This example shows how to use Amazon Simple Notification Service
/// (Amazon SNS) to add a new Amazon SNS topic.
/// </summary>
public class CreateSNSTopic
{
```

```
        public static async Task Main()
        {
            string topicName = "ExampleSNSTopic";

            IAmazonSimpleNotificationService client = new
 AmazonSimpleNotificationServiceClient();

            var topicArn = await CreateSNSTopicAsync(client, topicName);
            Console.WriteLine($"New topic ARN: {topicArn}");
        }

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

建立具有名稱、特定 FIFO 和重複資料刪除屬性的新主題。

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
```

```
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
 "true");
            }
        }

        var createResponse = await
 _amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考CreateTopic中的。

## C++

### 適用於 C++ 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }
```

```
    return outcome.IsSuccess();
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for C++ API 參考CreateTopic中的。

## CLI

### AWS CLI

建立 SNS 主題

下列 `create-topic` 範例會建立名為 `my-topic` 的 SNS 主題。

```
aws sns create-topic \
    --name my-topic
```

輸出：

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

如需詳細資訊，請參閱命 AWS 令列介面使用者指南中的 Amazon SQS 和 Amazon SNS 使用 AWS 命令列界面。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考CreateTopic中的。

## Go

### SDK for Go V2

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(topicName string, isFifoTopic bool,
 contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(context.TODO(), &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Go API 參考CreateTopic中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考CreateTopic中的。

## JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

在單獨的模組中建立用戶端並將其匯出。

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

匯入 SDK 和用戶端模組，然後呼叫 API。

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- 如需詳細資訊，請參閱《AWS SDK for JavaScript 開發人員指南》。
- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考CreateTopic中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK CreateTopic中的 Kotlin API 參考。

PHP

適用於 PHP 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
use Aws\Sns\SnsClient;
```

```
/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- 如需詳細資訊，請參閱《AWS SDK for PHP 開發人員指南》。
- 如需 API 詳細資訊，請參閱 AWS SDK for PHP API 參考CreateTopic中的。

## Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件CreateTopic中的 Python (博托 3) API 參考。

## Ruby

### 適用於 Ruby 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = "YourTopicName" # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts "The topic was not created. Stopping program."
    exit 1
  end
end
```

- 如需詳細資訊，請參閱《AWS SDK for Ruby 開發人員指南》。
- 如需 API 詳細資訊，請參閱 AWS SDK for Ruby API 參考CreateTopic中的。

## Rust

### 適用於 Rust 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- 如需 API 的詳細資訊，請參閱 AWS SDK CreateTopic中的 Rust API 參考資料。

## SAP ABAP

### 適用於 SAP ABAP 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    TRY.
        oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
 is returned for testing purposes. "
        MESSAGE 'SNS topic created' TYPE 'I'.
      CATCH /aws1/cx_snstopiclimitexcdex.
```

```
        MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- 如需 API 詳細資訊，請參閱 AWS SDK CreateTopic中的 SAP ABAP API 參考資料。

> **Note**
>
> 您也可以使用其他帳戶的 Amazon SNS 主題，但這樣就可能需要建立適用於該主題的政策，將存取許可授予 AWS Config。如需授予 Amazon SNS 主題許可的相關資訊，請參閱《Amazon SNS 主題的許可》，然後前往《建立 IAM 角色》。

## 建立 IAM 角色

### 使用 IAM 主控台

您可以使用 IAM 主控台建立 IAM 角色，以授與存取 Amazon S3 儲存貯體的 AWS Config 許可、存取 Amazon SNS 主題，以及取得支援 AWS 資源的組態詳細資料。當您使用主控台建立 IAM 角色時，AWS Config 會自動為您將必要的許可連接至角色。

> **Note**
>
> 如果您使用的 AWS 服務使用 AWS Config (例如 AWS Security Hub 或 AWS Control Tower)，且已建立 AWS Config 角色，則應確保您在設定時使用的 IAM 角色與已建立的角 AWS Config 色 AWS Config 保持相同的最低權限，以便其他 AWS 服務如預期般繼續執行。
> 例如，如果 AWS Control Tower 具有允 AWS Config 許讀取 Amazon S3 物件的 IAM 角色，則應確保在設定時使用的 IAM 角色中授予相同的許可 AWS Config。否則，可能會干擾 AWS 控制塔的運作。
> 如需的 IAM 角色的詳細資訊 AWS Config，請參閱 AWS Identity and Access Management。

### 若要建立 AWS 服務的角色

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。

3. 對於 Select trusted entity (選取信任的實體) 區段，選擇 AWS service (AWS 服務)。
4. 選擇您想要的使用案例 AWS Config：「組 Config-自訂」、「組 Config- Organizations」、「組 Config」或「組 Config-一致性套件」。然後選擇下一步。
5. 在 名稱、檢閱和建立 頁面中，檢閱角色的詳細資訊，然後選擇 建立角色。

## 使用 AWS 軟體開發套件

要使用 AWS SDK，您必須使用憑據對其進行配置。如需詳細資訊，請參閱 AWS SDK和工具參考指南中的共享的配置和認證文件。

下列程式碼範例會示範如何使用`CreateRole`。

### .NET

#### AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考CreateRole中的。

## Bash

### AWS CLI 與 bash 腳本

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.
```

```
# bashsupport disable=BP5008
function usage() {
  echo "function iam_create_user_access_key"
  echo "Creates an AWS Identity and Access Management (IAM) role."
  echo "  -n role_name   The name of the IAM role."
  echo "  -p policy_json -- The assume role policy document."
  echo ""
}

# Retrieve the calling parameters.
while getopts "n:p:h" option; do
  case "${option}" in
    n) role_name="${OPTARG}" ;;
    p) policy_document="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$role_name" ]]; then
  errecho "ERROR: You must provide a role name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$policy_document" ]]; then
  errecho "ERROR: You must provide a policy document with the -p parameter."
  usage
  return 1
fi

response=$(aws iam create-role \
  --role-name "$role_name" \
  --assume-role-policy-document "$policy_document" \
  --output text \
```

```
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考CreateRole中的。

## C++

適用於 C++ 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
```

```
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for C++ API 參考CreateRole中的。

## CLI

### AWS CLI

範例 1：建立 IAM 角色

下列 `create-role` 命令會建立名為 `Test-Role` 的角色，並將信任政策連接至該角色。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

輸出：

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

在 Test-Role-Trust-Policy.json 檔案中，將信任政策定義為 JSON 文件。(檔案名稱和副檔名沒有意義。) 信任政策必須指定主體。

若要將許可政策連接至角色，請使用 `put-role-policy` 命令。

如需詳細資訊，請參閱《AWS IAM 使用者指南》中的建立 IAM 角色。

範例 2：建立具有指定最長工作階段持續時間的 IAM 角色

下列 `create-role` 命令會建立名為 `Test-Role` 的角色，並設定 7200 秒 (2 小時) 的最長工作階段持續時間。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

輸出：

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

如需詳細資訊，請參閱《AWS IAM 使用者指南》中的修改角色最長工作階段持續時間 (AWS API)。

範例 3：建立內含標籤的 IAM 角色

下列命令會建立內含標籤的 IAM 角色 `Test-Role`。此範例使用具有下列 JSON 格式標記的 `--tags` 參數旗標：`'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`。或者，`--tags` 旗標可以與速記格式的標籤一起使用：`'Key=Department,Value=Accounting Key=Location,Value=Seattle'`。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

輸出：

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
```

```
        ]
    }
}
```

如需詳細資訊，請參閱《AWS IAM 使用者指南》中的標記 IAM 角色。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考CreateRole中的。

## Go

### SDK for Go V2

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(roleName string, trustedUserArn string)
 (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version:   "2012-10-17",
  Statement: []PolicyStatement{{
   Effect: "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
```

```
    Action: []string{"sts:AssumeRole"},
   }},
  }
  policyBytes, err := json.Marshal(trustPolicy)
  if err != nil {
   log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
  trustedUserArn, err)
   return nil, err
  }
  result, err := wrapper.IamClient.CreateRole(context.TODO(),
  &iam.CreateRoleInput{
   AssumeRolePolicyDocument: aws.String(string(policyBytes)),
   RoleName:                 aws.String(roleName),
  })
  if err != nil {
   log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
  } else {
   role = result.Role
  }
  return role, err
 }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Go API 參考CreateRole中的。

## Java

### 適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
```

```
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
 represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
```

```
    }

    public static String createIAMRole(IamClient iam, String rolename, String
 fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
 readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
 response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }

    public static Object readJsonSimpleDemo(String filename) throws Exception {
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考CreateRole中的。

## JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

建立角色。

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考CreateRole中的。

## PHP

適用於 PHP 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for PHP API 參考CreateRole中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會建立名為的新角色，**MyNewRole**並將檔案中找到的原則附加至該角色**NewRoleTrustPolicy.json**。請注意，您必須使用 **-Raw** switch 參數才能成功處理 JSON 原則檔案。輸出中顯示的策略文件經過 URL 編碼。它在這個例子中使用 **UrlDecode** .NET 方法進行解碼。

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

輸出：

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
RoleId                   : V5PAJI2KPN4EAEXAMPLE1
RoleName                 : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程CreateRole式參考中的。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
```

```
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件CreateRole中的 Python (博托 3) API 參考。

## Ruby

適用於 Ruby 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
```

```
      )
    end

    role_arn
  rescue Aws::IAM::Errors::ServiceError => e
    @logger.error("Error creating role: #{e.message}")
    nil
  end
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Ruby API 參考CreateRole中的。

## Rust

### 適用於 Rust 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- 如需 API 的詳細資訊，請參閱 AWS SDK CreateRole中的 Rust API 參考資料。

## Swift

### 適用於 Swift 的 SDK

> **Note**
>
> 這是適用於預覽版本 SDK 的發行前版本文件。內容可能變動。

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public func createRole(name: String, policyDocument: String) async throws ->
String {
       let input = CreateRoleInput(
           assumeRolePolicyDocument: policyDocument,
           roleName: name
       )
       do {
           let output = try await client.createRole(input: input)
           guard let role = output.role else {
               throw ServiceHandlerError.noSuchRole
           }
           guard let id = role.roleId else {
               throw ServiceHandlerError.noSuchRole
           }
           return id
       } catch {
           throw error
       }
   }
```

- 有關 API 的詳細信息，請參閱 AWS SDK CreateRole中的斯威夫特 API 參考。

## 從 AWS Config 開始 AWS CLI

> **Note**
>
> 在設 AWS Config 定之前 AWS CLI，您需要建立 S3 儲存貯體、SNS 主題以及具有附加政策的 IAM 角色做為先決條件。然後，您可以使用 AWS CLI 來指定的值區、主題和角色 AWS Config。若要設定的先決條件 AWS Config，請參閱先決條件。

若要開 AWS Config 始 AWS CLI，請使用輸入配置記錄器、放入傳送通道和開始-配置-記錄器指令，如下所示：

- `put-configuration-recorder` 命令會建立新的組態記錄器，記錄您指定的資源組態。
- `put-delivery-channel` 命令會建立交付通道物件，將組態資訊交付給 S3 儲存貯體和 SNS 主題。
- 建立交付通道後，`start-configuration-recorder` 會開始記錄您選取的資源組態，您可以在 AWS 帳戶中看到這些組態。

> **Note**
>
> 您帳戶中的每個 AWS 區域都只能擁有一部組態記錄器和一個交付通道。

您可以指定記錄器的名稱和 IAM 角色的 Amazon 資源名稱 (ARN)，由組態錄製程式承擔 AWS Config 並使用。 AWS Config 建立組態記錄器時，會自動指定「default」的名稱。組態記錄器建立之後即無法變更名稱。若要變更組態記錄器的名稱，您必須刪除它，再使用新的名稱建立新的組態記錄器。

若要使 AWS Config 用設定多帳戶多區域資料彙總 AWS CLI，請參閱使用 AWS 命令列介面設定彙總器。您必須為每個您想要記錄組態項目的每 AWS 帳戶 個區域建立個別的組態記錄程式。

內容

- put-configuration-recorder
- put-delivery-channel
- start-configuration-recorder

## put-configuration-recorder

您的 put-configuration-recorder 命令看起來應如以下範例。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

此指令會使用`--configuration-recorder`和`---recording-group`欄位。

> **Note**
>
> 錄音組和配置記錄器
> `--recording-group` 欄位指定記錄的資源類型。
> 此`--configuration-recorder`欄位會指定name組態錄製程式的預設錄製頻率，以及(`recordingMode`)。`roleArn`您也可以使用此欄位覆寫特定資源類型的記錄頻率。

### 記錄群組

put-configuration-recorder 會使用下列適用於 `--recording-group` 參數的選項：

- `allSupported=true`— AWS Config 記錄所有支援資源類型的組態變更，不包括全域 IAM 資源類型。新 AWS Config 增對新資源類型的支援時， AWS Config 會自動開始記錄該類型的資源。
- `includeGlobalResourceTypes=true` – 此選項為搭售方案，僅適用於全域的 IAM 資源類型：IAM 使用者、群組、角色和客戶管理政策。這些全球 IAM 資源類型只能在 2022 年 2 月之前提供的 AWS Config 區域 AWS Config 中進行記錄。您無法在 2022 年 2 月 AWS Config 之後支援的區域中記錄全球 IAM 資源類型。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

> **Important**
>
> Aurora 全域叢集會記錄在所有啟用的區域中
> 資`AWS::RDS::GlobalCluster`源類型將記錄在啟用組態記錄程式的所有支援 AWS Config 區域中，即使設定為也`includeGlobalResourceTypes`是如此`false`。此 `includeGlobalResourceTypes` 選項是僅適用於 IAM 使用者、群組、角色和客戶管理政策的配套。
> 如果不希望在所有已啟用的區域中記錄 `AWS::RDS::GlobalCluster`，請使用下列一種記錄策略：

1. 記錄所有目前和未來的資源類型 (附帶排除項目) (EXCLUSION_BY_RESOURCE_TYPES)，或
2. 記錄特定資源類型 (INCLUSION_BY_RESOURCE_TYPES)。

如需詳細資訊，請參閱《選取要記錄的資源》。

**Important**

包括GlobalResourceTypes 和排除記錄策略

該includeGlobalResourceTypes字段對EXCLUSION_BY_RESOURCE_TYPES記錄策略沒有影響。這表示在設定為exclusionByResourceTypes時includeGlobalResourceTypes，不會自動將全域 IAM 資源類型 (IAM 使用者、群組、角色和客戶受管政策) 新增為排除項false。

此includeGlobalResourceTypes欄位只應用於修改AllSupported欄位，因為欄位的預設值是記錄所有受支援資源類型 (不包括全AllSupported域 IAM 資源類型) 的組態變更。若要在設定為時AllSupported包含全域 IAM 資源類型true，請務必將設定includeGlobalResourceTypes為true。

若要排除EXCLUSION_BY_RESOURCE_TYPES記錄策略的全域 IAM 資源類型，您需要手動將它們新增到的resourceTypes欄位exclusionByResourceTypes。

**Note**

必要欄位和選用欄位

在將 includeGlobalResourceTypes 設定為 true 之前，請先將 allSupported 欄位設定為 true。

或者，也可以將 RecordingStrategy 的 useOnly 欄位設定為 ALL_SUPPORTED_RESOURCE_TYPES。

**Note**

覆寫欄位

如果在的欄位中設定includeGlobalResourceTypes為false但列出全域 IAM 資源類型 RecordingGroup，則無論您是否 AWS Config 將resourceTypes欄位設定為 false，仍會記錄這些指定資源類型的includeGlobalResourceTypes組態變更。

如果您不想記錄全域 IAM 資源類型 (IAM 使用者、群組、角色和客戶管理政策) 的組態變更，除了將 `includeGlobalResourceTypes` 欄位設定為 false 之外，請切勿在 `resourceTypes` 欄位中列出這些類型。

- `recordingStrategy` - 指定組態記錄器的記錄策略。`recordingGroup.json` 檔案會指定 AWS Config 記錄的資源類型：
  - 如果將`useOnly`欄位設定RecordingStrategy為`ALL_SUPPORTED_RESOURCE_TYPES`，則會 AWS Config 記錄所有支援資源類型的組態變更，不包括全域 IAM 資源類型。或者，您可以RecordingGroup將的`allSupported`欄位設定為`true`。新 AWS Config 增對新資源類型的支援時， AWS Config 會自動開始記錄該類型的資源。
  - 如果RecordingStrategy將的`useOnly`欄位設定為`INCLUSION_BY_RESOURCE_TYPES`，則只會針對您在的欄`resourceTypes`位中指定的資源類型 AWS Config 記錄組態變更RecordingGroup。
  - 如果RecordingStrategy將的`useOnly`欄位設定為`EXCLUSION_BY_RESOURCE_TYPES`，則會 AWS Config 記錄所有支援資源類型的組態變更，但您指定為排除在的`resourceTypes`欄位中不記錄的資源類型除外ExclusionByResourceTypes。

> **Note**
>
> 必要欄位和選用欄位
>
> 當您將 `--recording-group` 的 `allSupported` 欄位設定為 `true` 時，`recordingStrategy` 欄位為選用。
>
> 當您在 `--recording-group` 的 `resourceTypes` 欄位中列出資源類型時，`recordingStrategy` 欄位為選用。
>
> 如果您在 `exclusionByResourceTypes` 的 `resourceTypes` 欄位中列出要排除記錄的資源類型，則 `recordingStrategy` 欄位為必要。

> **Note**
>
> 覆寫欄位
>
> 如果記錄策略選擇 `EXCLUSION_BY_RESOURCE_TYPES`，則 `exclusionByResourceTypes` 欄位會覆寫請求中的其他屬性。
>
> 例如，除非您在 `exclusionByResourceTypes` 的 `resourceTypes` 欄位中特別將全域 IAM 資源類型列為豁免項目，否則即使將 `includeGlobalResourceTypes` 設為 false，此選項仍會自動記錄這些資源類型。

> **Note**
>
> 全域資源類型和資源排除記錄策略
>
> 依預設，如果您選擇`EXCLUSION_BY_RESOURCE_TYPES`記錄策略，則當您在設定組態記錄程式的區域 (包括全域資源類型) 中新 AWS Config 增對新資源類型的支援時，會自動 AWS Config 開始記錄該類型的資源。
>
> 除非特別列為排除項目，否則在啟用組態記錄程式後，所有支援的 AWS Config 區域都`AWS::RDS::GlobalCluster`會自動記錄。
>
> IAM 使用者、群組、角色和客戶受管政策會記錄在您設定組態記錄器的區域 (如果該區域是 2022 年 2 月之前提供服務的區域)。 AWS Config 您無法在 2022 年 2 月 AWS Config 之後支援的區域中記錄全球 IAM 資源類型。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

以下顯示 `recordingGroup.json` 的請求語法。

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

> **Note**
>
> AWS Organizations 可以防止存取的授權原則
>
> 如果您使用預先存在的 IAM 角色，請確保沒有授權政策阻 AWS Config 止您記錄資源的權限。 AWS Organizations 如需有關的授權原則的詳細資訊 AWS Organizations，請參閱《AWS Organizations 使用指南》AWS Organizations中的〈管理策略〉。
>
> 重複使用 IAM 角色時保持最低權限
>
> 如果您使用的 AWS 服務使用 AWS Config，例如 AWS Security Hub 或 AWS Control Tower，且已建立 IAM 角色，請確保您在設定時使用的 IAM 角色保 AWS Config 持與預先

存在的 IAM 角色相同的最低許可。您必須這麼做，以確保其他 AWS 服務能如預期般繼續執行。
例如，如果 AWS Control Tower 具有允許 AWS Config 讀取 S3 物件的 IAM 角色，請確保將相同的許可授與您在設定時使用的 IAM 角色 AWS Config。否則，它可能會干擾 AWS Control Tower 操作方式。

> **Note**
>
> 大量的 AWS Config 評估
> 與之後的月份相比，您可能會注意到在使用 AWS Config 錄製首個月期間帳戶中的活動有所增加。在初始啟動安裝程序期間， AWS Config 會對 AWS Config 您帳戶中選取要記錄的所有資源執行評估。
> 如果您正在執行暫時工作負載，您可能會看到活動增加， AWS Config 因為它會記錄與建立和刪除這些暫時資源相關聯的組態變更。暫時性工作負載是暫時使用因需要而載入和執行的運算資源。範例包括 Amazon 彈性運算雲端 (Amazon EC2) 競價型執行個體、亞馬遜 EMR 任務和 AWS Auto Scaling. 如果您想要避免因執行臨時工作負載而增加的活動，您可以設定組態錄製程式以將這些資源類型排除在記錄之外，或在關 AWS Config 閉的情況下在單獨的帳戶中執行這些類型的工作負載，以避免增加組態記錄和規則評估。

> **Note**
>
> 區域可用性
> 在指定 AWS Config 要追蹤的資源型態之前，請先勾選「依可用區域的資源涵蓋範圍」，以查看您要設定的「 AWS 區域」中是否支援資源型態 AWS Config。如果至少一個「區域」支援某個資源類型，則您可以 AWS Config 在所支援的所有「區域」中啟用該資源類型的記錄 AWS Config，即使您要設定的「 AWS 區域」不支援指定的資源類型也一樣 AWS Config。

組態記錄器

`put-configuration-recorder` 會使用下列用於 `--configuration-recorder` 參數的欄位：

- `name`— 組態記錄程式的名稱。 AWS Config 建立組態記錄器時，會自動指定「default」的名稱。
- `roleARN`— 由組態記錄器承擔 AWS Config 並使用之 IAM 角色的 Amazon 資源名稱 (ARN)。

- `recordingMode`— 指定用來記錄組態變更的預設錄製頻率。 AWS Config AWS Config 支持連續錄製和每日錄製。連續記錄可讓您在發生變更時持續記錄組態變更。每日記錄可讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。
  - `recordingFrequency`— AWS Config 用來記錄組態變更的預設錄製頻率。

    > **Note**
    >
    > AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

  - `recordingModeOverrides` — 此欄位可讓您指定記錄模式的覆寫。其為 `recordingModeOverride` 物件的陣列。`recordingModeOverrides` 陣列中的每個 `recordingModeOverride` 物件都包含三個欄位：
    - `description` — 您為覆寫提供的描述。
    - `recordingFrequency` — 會套用至覆寫中指定的所有資源類型的記錄頻率。
    - `resourceTypes`— 以逗號分隔的清單，指定覆寫中 AWS Config 包含哪些資源類型。

> **Note**
>
> 必要欄位和選用欄位
> put-configuration-recorder 的 `recordingMode` 欄位為選用。依預設，組態記錄器的記錄頻率設定為連續記錄。

> **Note**
>
> 限制
> 下列資源類型不支援每日記錄：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> 對於記錄所有目前和未來支援的資源類型 (`ALL_SUPPORTED_RESOURCE_TYPES`) 記錄策略，這些資源類型會設定為「連續記錄」。

configurationRecorder.json檔案會指定name組態錄製程式的預設錄製頻率，以及(recordingMode)。roleArn您也可以使用此欄位覆寫特定資源類型的記錄頻率。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

## put-delivery-channel

下列程式碼範例會示範如何使用PutDeliveryChannel。

### CLI

#### AWS CLI

若要建立傳送管道

下列命令會以 JSON 程式碼的形式提供傳遞通道的設定：

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

deliveryChannel.json檔案會指定傳送通道屬性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
```

```
}
```

此範例會設定下列屬性：

name-傳送管道的名稱。根據預設， AWS Config 會將名稱`default`指派給新的傳送通道。您無法使用指令更新傳送通道名稱。`put-delivery-channel`如需變更名稱的步驟，請參閱重新命名傳遞管道。 `s3BucketName`-Con AWS fig 交付組態快照和組態歷史記錄檔案的 Amazon S3 儲存貯體的名稱。如果您指定屬於另一個 AWS 帳戶的儲存貯體，則該儲存貯體必須具有授與 Config 存取權限的政策。 AWS 如需詳細資訊，請參閱《Amazon S3 儲存貯體許可》。

`snsTopicARN`-Amazon Amazon SNS 主題的 Amazon 資源名稱 (ARN)，組態會向其傳送有關組態變更的通知。如果您從其他帳戶選擇主題，則該主題必須具有授與 AWS Config 存取權限的政策。 AWS 如需詳細資訊，請參閱 Amazon SNS 主題的許可。

`configSnapshotDeliveryProperties`-包含`deliveryFrequency`屬性，可設定 AWS Config 傳送組態快照的頻率，以及呼叫週期性組 Config 規則評估的頻率。

如果命令成功， AWS Config 不會返回任何輸出。若要驗證傳遞通道的設定，請執行 describe-delivery-channels 命令。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考中的PutDelivery頻道。

PowerShell

適用的工具 PowerShell

範例 1：此範例會變更現有傳送管道的傳送頻率屬性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程式參考中的PutDelivery通道。

## start-configuration-recorder

若要完成開啟 AWS Config，請使用`start-configuration-recorder`指令。

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

# 驗證 AWS Config 是否已成功啟動 AWS CLI

啟動之後 AWS Config，您可以使用 AWS CLI 命令來檢查是否正在執行，以及 AWS Config 是否 AWS Config 已建立組態記錄程式和傳遞通道。您也可以確認是否 AWS Config 已開始記錄並將組態傳送至傳送管道。

內容


- 確認交付通道已建立
- 確認組態記錄器已建立
- 檢查是否 AWS Config 已開始錄製


## 確認交付通道已建立

使用 `describe-delivery-channels` 命令確認已設定您的 Amazon S3 儲存貯體及 Amazon SNS 主題。

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

當您使用 CLI、服務 API 或 SDK 設定傳遞通道且未指定名稱時， AWS Config 會自動指派名稱 `"default"`。

## 確認組態記錄器已建立

使用 `describe-configuration-recorders` 命令確認組態記錄器已建立，且該組態記錄器擔任 IAM 角色。如需詳細資訊，請參閱 建立 IAM 角色。

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
```

```
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

### 檢查是否 AWS Config 已開始錄製

使用命describe-configuration-recorder-status令檢查是否 AWS Config 已開始記錄您帳戶中現有支援 AWS 資源的組態。記錄的組態會交付至指定的交付通路。

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

`recording` 欄位中的值 `true` 會確認組態記錄器已開始記錄您所有資源的組態。 AWS Config 會使用 UTC 格式記錄時間。輸出顯示為 Unix 時間戳記。

如需查詢您帳戶中現有資源及了解您資源組態的資訊，請參閱檢視 資源組態和歷史記錄。

## 搭 AWS Config 配 AWS SDK 使用

AWS 軟件開發套件（SDK）可用於許多流行的編程語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

| SDK 文件 | 代碼範例 |
| --- | --- |
| AWS SDK for C++ | AWS SDK for C++ 程式碼範例 |

| SDK 文件 | 代碼範例 |
| --- | --- |
| AWS CLI | AWS CLI 程式碼範例 |
| AWS SDK for Go | AWS SDK for Go 程式碼範例 |
| AWS SDK for Java | AWS SDK for Java 程式碼範例 |
| AWS SDK for JavaScript | AWS SDK for JavaScript 程式碼範例 |
| 適用於 Kotlin 的 AWS SDK | 適用於 Kotlin 的 AWS SDK 程式碼範例 |
| AWS SDK for .NET | AWS SDK for .NET 程式碼範例 |
| AWS SDK for PHP | AWS SDK for PHP 程式碼範例 |
| AWS Tools for PowerShell | PowerShell 程式碼範例的工具 |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) 程式碼範例 |
| AWS SDK for Ruby | AWS SDK for Ruby 程式碼範例 |
| 適用於 Rust 的 AWS SDK | 適用於 Rust 的 AWS SDK 程式碼範例 |
| 適用於 SAP ABAP 的 AWS SDK | 適用於 SAP ABAP 的 AWS SDK 程式碼範例 |
| 適用於 Swift 的 AWS SDK | 適用於 Swift 的 AWS SDK 程式碼範例 |

可用性範例

找不到所需的內容嗎？ 請使用本頁面底部的提供意見回饋連結申請程式碼範例。

# 管理組態記錄器

AWS Config 使用組態記錄程式偵測資源組態中的變更，並將這些變更擷取為組態項目。您必須先建立組態記錄程式，才 AWS Config 能追蹤資源組態。當您啟動組態錄製程式 AWS Config 時，會清查您帳戶中的所有 AWS 資源。

每個 AWS 區域只能有一個組態記錄器通道 AWS 帳戶，而且需要使用交付通道 AWS Config。

如果您使用主控台或 AWS CLI 進行設 AWS Config 定，則 AWS Config 會自動為您建立組態錄製程式，然後啟動組態錄製程式。如需詳細資訊，請參閱 開始使用 AWS Config。

根據預設，組態記錄器會記錄所有 AWS Config 執行區域中支援的資源。您可以建立自訂組態記錄器，只記錄您指定的資源類型。如需詳細資訊，請參閱 錄製 AWS 資源。

AWS Config 開始錄製配置時，您需要支付服務使用費。如需定價資訊，請參閱 AWS Config 定價。

> **Important**
>
> 如果組態記錄器已關閉，則已刪除之資源的評估結果可以持續存在
> 如果組態錄製程式已關閉，則會停用追蹤資源組態變更 (包括其刪除) 的功能。 AWS Config 這表示如果關閉組態記錄器，您可能會看到先前刪除之資源的評估結果。

## 管理組態記錄器 (主控台)

您可以使用 AWS Config 控制台停止或啟動配置記錄器。您也可以變更組態記錄器的記錄頻率。

To stop or start the configuration recorder

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在導覽窗格中選擇 Settings (設定)。
3. 停止或啟動組態記錄器：
   - 若您希望停止記錄，請在 Recording is on (記錄已開啟) 下方，選擇 Turn off (關閉)。出現提示時，請選擇 繼續。
   - 若您希望開始記錄，請在 Recording is off (記錄已關閉) 下方，選擇 Turn on (開啟)。出現提示時，請選擇 繼續。

To change the recording frequency

AWS Config 支持連續錄製和每日錄製。連續記錄可讓您在發生變更時持續記錄組態變更。每日記錄可讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。如需詳細資訊，請參閱記錄頻率。

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在導覽窗格中選擇 Settings (設定)。
3. 選擇編輯以查看「記錄頻率」下的選項。

# 管理組態記錄器 (AWS CLI)

您可以使用停 AWS CLI 止或啟動組態錄製程式。您也可以使用 AWS Config API 或其中一個 AWS SDK 來 AWS CLI重新命名或刪除組態記錄程式。下列步驟可協助您使用 AWS CLI。

To stop the configuration recorder

使用 `stop-configuration-recorder` 命令：

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

To start the configuration recorder

使用 `start-configuration-recorder` 命令：

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

To change the recording frequency

使用 `put-configuration-recorder` 命令變更組態記錄器的記錄頻率：

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

`configurationRecorder.json`檔案會指定`name`組態錄製程式的預設錄製頻率，以及 (`recordingMode`)。`roleArn`您也可以使用此欄位覆寫特定資源類型的記錄頻率。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

put-configuration-recorder 會使用下列用於 `--configuration-recorder` 參數的欄位：

- name— 組態記錄程式的名稱。 AWS Config 建立組態記錄器時，會自動指定「default」的名稱。
- roleARN— 由組態記錄器承擔 AWS Config 並使用之 IAM 角色的 Amazon 資源名稱 (ARN)。
- recordingMode— 指定用來記錄組態變更的預設錄製頻率。 AWS Config AWS Config 支持連續錄製和每日錄製。連續記錄可讓您在發生變更時持續記錄組態變更。每日記錄可讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。
  - recordingFrequency— AWS Config 用來記錄組態變更的預設錄製頻率。

    > **Note**
    > AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

  - recordingModeOverrides — 此欄位可讓您指定記錄模式的覆寫。其為 recordingModeOverride 物件的陣列。recordingModeOverrides 陣列中的每個 recordingModeOverride 物件都包含三個欄位：
    - description — 您為覆寫提供的描述。
    - recordingFrequency — 會套用至覆寫中指定的所有資源類型的記錄頻率。
    - resourceTypes— 以逗號分隔的清單，指定覆寫中 AWS Config 包含哪些資源類型。

> **Note**
>
> 必要欄位和選用欄位
>
> put-configuration-recorder 的 recordingMode 欄位為選用。依預設，組態記錄器的記錄頻率設定為連續記錄。

> **Note**
>
> 限制
>
> 下列資源類型不支援每日記錄：
>
> - AWS::Config::ResourceCompliance
> - AWS::Config::ConformancePackCompliance
> - AWS::Config::ConfigurationRecorder
>
> 對於記錄所有目前和未來支援的資源類型 (ALL_SUPPORTED_RESOURCE_TYPES) 記錄策略，這些資源類型會設定為「連續記錄」。

To delete the configuration recorder

使用 delete-configuration-recorder 命令：

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To rename the configuration recorder

若要變更組態記錄器的名稱，您必須刪除它並使用您需要的名稱建立新的組態記錄器。

1. 使用 describe-configuration-recorders 命令查詢您目前組態記錄器的名稱：

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
```

```
        }
    ]
}
```

2. 使用 delete-configuration-recorder 命令刪除您目前的組態記錄器：

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. 使用 put-configuration-recorder 命令，使用需要的名稱建立組態記錄器：

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. 使用 start-configuration-recorder 命令繼續記錄：

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

# 組態記錄器的漂移偵測

`AWS::Config::ConfigurationRecorder` 資源類型是組態記錄器的組態項目 (CI)，可追蹤組態記錄器狀態的所有變更。您可以使用此 CI 來檢查組態記錄器的狀態是否與先前狀態不同，或已漂移。例如，此 CI 會追蹤您已啟用追蹤的資源類型更新、是否已停止或啟 AWS Config 動組態錄製程式，或者您是否已刪除或解除安裝組態錄製程式。已漂移的組態記錄器會指出您未準確偵測預期資源類型的變更。如果您的組態記錄器已經漂移，這可能會導致誤判為非或誤判為真的合規結果。

資`AWS::Config::ConfigurationRecorder`源類型是系統資源類型， AWS Config 且此資源類型的記錄預設會在所有支援的區域中啟用。`AWS::Config::ConfigurationRecorder` 資源型態的記錄不會收取額外的費用。

# 管理交付管道

隨著 AWS Config 持續記錄 AWS 資源發生的變更，它會透過傳遞通道傳送通知和更新的組態狀態。您可以管理傳遞通道，以控制 AWS Config 傳送組態更新的位置。

每個 AWS 區域每個區域只能有一個傳遞通道 AWS 帳戶，而且必須使用交付通道 AWS Config。

當 AWS Config 偵測到資源的組態變更，且通知超過 Amazon SNS 允許的大小上限時，通知會包含組態項目的簡短摘要。您可以在 `s3BucketLocation` 欄位所指定的 Amazon S3 儲存貯體位置檢視完整通知。如需詳細資訊，請參閱《範例大型組態項目變更通知》。

> **Note**
>
> AWS Config 支援 AWS KMS 加密所使用的 Amazon S3 儲存貯體 AWS Config
> 您可以提供 AWS Key Management Service (AWS KMS) 金鑰或別名 Amazon 資源名稱 (ARN)，以加密傳送到 Amazon Simple Storage Service (Amazon S3) 貯體的資料。根據預設，會將組態歷史記錄和快照檔案 AWS Config 交付到您的 Amazon S3 儲存貯體，並使用 S3 AES-256 伺服器端加密 SSE-S3 加密靜態資料。不過，如果您提 AWS Config 供 KMS 金鑰或別名 ARN，則 AWS Config 會使用該 KMS 金鑰而非 AES-256 加密。
> AWS Config 不支援將通道交付到已啟用物件鎖定且啟用預設保留的 Amazon S3 儲存貯體。如需詳細資訊，請參閱 S3 物件鎖定的運作方式。

主題


- 術語
- 更新交付管道
- 重新為交付管道命名
- 組態項目的元件
- 將組態快照交付到 Amazon S3 儲存貯體
- AWS Config 傳送至 Amazon SNS 主題的通知


## 術語

組態項目代表您帳號中存在之受支援 AWS 資源的各種屬性的 point-in-time 檢視。組態項目的元件包括中繼資料、屬性、關係、目前的組態及相關事件。 AWS Config 每當它偵測到它正在記錄的資源類型

的變更時，就會建立組態項目。例如，如果 AWS Config 要記錄 Amazon S3 儲存貯體，則在建 AWS Config 立、更新或刪除儲存貯體時建立組態項目。您也可以選擇為 AWS Config 以您設定的錄製頻率建立組態項目。

組態歷史記錄是指定資源在任何時間期間的組態項目集合。組態歷史記錄可協助您回答下列這類問題，例如，第一次建立資源時、上個月如何設定資源，以及昨天 9 AM 進行何種組態變更。您可以使用多種格式的組態歷程記錄。 AWS Config 針對要記錄到您指定的 Amazon S3 儲存貯體的每個資源類型，自動交付組態歷史記錄檔案。您可以在 AWS Config 主控台中選取指定的資源，並使用時間軸瀏覽至該資源的所有先前設定項目。此外，您也可以從 API 存取資源的歷史組態項目。

組態快照是帳戶中現有所支援資源的組態項目集合。此組態快照是所記錄資源和其組態的完整全貌。組態快照可以是驗證組態的實用工具。例如，建議您定期檢查未正確設定或可能不存在之資源的組態快照。組態快照具有多種格式。您可以將組態快照交付至您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。此外，您可以在 AWS Config 主控台中選取時間點，並使用資源之間的關係瀏覽組態項目的快照集。

配置流是一個自動更新的列表，其中包含 AWS Config 正在記錄的資源的所有配置項目。每次建立、修改或刪除資源時， AWS Config 都會建立組態項目，並新增至組態串流。使用您選擇的 Amazon Simple Notification Service (Amazon SNS) 主題後，組態串流即可運作。配置流有助於觀察發生的配置更改，以便您發現潛在問題，在某些資源發生變更時產生通知，或更新需要反映 AWS 資源配置的外部系統。

# 更新交付管道

在您更新交付管道時，您可以設定下列選項：

- AWS Config 傳送組態快照和組態歷史記錄檔案的 Amazon S3 儲存貯體。
- 將組態快照 AWS Config 交付到 Amazon S3 儲存貯體的頻率。
- AWS Config 傳送有關組態變更通知的 Amazon SNS 主題。

## 更新傳送通道（主控台）

您可以使用主 AWS Config 控台為交付通道設定 Amazon S3 儲存貯體和 Amazon SNS 主題。如需管理這些設定的步驟，請參閱使用主控 AWS Config 台進行設定。

主控台不會提供重新命名交付管道、設定組態快照頻率，或是刪除交付管道的選項。若要執行這些工作 AWS CLI，您必須使用 AWS Config API 或其中一個 AWS SDK。

## 若要更新傳遞管道 (AWS SDK)

下列程式碼範例會示範如何使用`PutDeliveryChannel`。

CLI

AWS CLI

若要建立傳送管道

下列命令會以 JSON 程式碼的形式提供傳遞通道的設定：

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

`deliveryChannel.json`檔案會指定傳送通道屬性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

此範例會設定下列屬性：

name-傳送管道的名稱。根據預設， AWS Config 會將名稱`default`指派給新的傳送通道。您無法使用指令更新傳送通道名稱。`put-delivery-channel`如需變更名稱的步驟，請參閱重新命名傳遞管道。 `s3BucketName`-Con AWS fig 交付組態快照和組態歷史記錄檔案的 Amazon S3 儲存貯體的名稱。如果您指定屬於另一個 AWS 帳戶的儲存貯體，則該儲存貯體必須具有授與 Config 存取權限的政策。 AWS 如需詳細資訊，請參閱《Amazon S3 儲存貯體許可》。

`snsTopicARN`-Amazon Amazon SNS 主題的 Amazon 資源名稱 (ARN)，組態會向其傳送有關組態變更的通知。如果您從其他帳戶選擇主題，則該主題必須具有授與 AWS Config 存取權限的政策。 AWS 如需詳細資訊，請參閱 Amazon SNS 主題的許可。

`configSnapshotDeliveryProperties`-包含`deliveryFrequency`屬性，可設定 AWS Config 傳送組態快照的頻率，以及呼叫週期性組 Config 規則評估的頻率。

如果命令成功， AWS Config 不會返回任何輸出。若要驗證傳送通道的設定，請執行 describe-delivery-channels 命令。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考中的PutDelivery頻道。

PowerShell

適用的工具 PowerShell

範例 1：此範例會變更現有傳送管道的傳送頻率屬性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程式參考中的PutDelivery通道。

(選擇性) 您可以使用 `describe-delivery-channels` 命令確認交付管道設定已更新：

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

下列程式碼範例會示範如何使用`DescribeDeliveryChannels`。

CLI

AWS CLI

取得有關傳送管道的詳細資訊

下列命令會傳回有關傳送通道的詳細資料：

```
aws configservice describe-delivery-channels
```

輸出：

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考中的DescribeDelivery頻道。

PowerShell

適用的工具 PowerShell

範例 1：此範例會擷取區域的傳送管道並顯示詳細資訊。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

輸出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程式參考中的DescribeDelivery通道。

# 重新為交付管道命名

若要變更交付管道的名稱，您必須刪除它並使用您需要的名稱建立新的交付管道。您必須暫時停止組態記錄器，才能刪除交付管道。

主 AWS Config 控台未提供刪除傳遞通道的選項，因此您必須使用 AWS CLI、 AWS Config API 或其中一個 AWS SDK。

## 重新命名交付管道 (AWS CLI)

使用重新命名傳送管道 AWS CLI

1. 使用 stop-configuration-recorder 命令停止組態記錄器：

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. 使用 describe-delivery-channels 命令並記下您交付管道的屬性：

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. 使用 delete-delivery-channel 命令刪除交付管道：

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. 使用 put-delivery-channel 命令，使用需要的名稱建立交付管道：

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

deliveryChannel.json 檔案指定了交付管道屬性：

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
```

```
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. 使用 `start-configuration-recorder` 命令繼續記錄：

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

# 組態項目的元件

組態項目代表您帳號中存在之受支援 AWS 資源的各種屬性的 point-in-time 檢視。組態項目的元件包括中繼資料、屬性、關係、目前的組態及相關事件。 AWS Config 每當它偵測到它正在記錄的資源類型的變更時，就會建立組態項目。例如，如果 AWS Config 要記錄 Amazon S3 儲存貯體，則在建 AWS Config 立、更新或刪除儲存貯體時建立組態項目。您也可以選擇為 AWS Config 以您設定的錄製頻率建立組態項目。

組態項目由下列元件組成。

| 元件 | 描述 | 包含 |
| --- | --- | --- |
| 中繼資料 | 此組態項目的相關資訊 | • 版本 ID<br>• 擷取此組態項目的時間<br>• 組態項目的狀態，指出是否成功擷取項目<br>• 狀態 ID，指出資源組態項目的順序 |
| Attributes | 資源屬性 | • 資源 ID<br>• 此資源的金鑰/值標籤清單<br>• 資源類型 (請參閱支援的資源類型)<br>• Amazon Resource Name (ARN)<br>• 包含資源的可用區域 (若適用)<br>• 建立資源的時間 |

| 元件 | 描述 | 包含 |
| --- | --- | --- |
| 關係 | 資源與其他和帳戶建立關聯之資源的相關方式 | 關係的描述，例如 Amazon EBS 磁碟區 `vol-1234567` 連接到 Amazon EC2 執行個體 `i-a1b2c3d4` |
| 目前的組態 | 透過呼叫資源的 Describe 或 List API 傳回的資訊 | 例如，`DescribeVolumes` API 會傳回下列磁碟區的相關資訊：<br>• 磁碟區所在的可用區域<br>• 磁碟區連接的時間<br>• 其連接到的 EC2 執行個體 ID<br>• 磁碟區的目前狀態<br>• DeleteOnTermination 国旗的状态<br>• 磁碟區連接的裝置<br>• 磁碟區類型，例如 `gp2`, `io1`, 或 `standard` |

備註

1. 組態項目關聯不包含網路流程或資料流程依存。組態項目無法經由自訂以代表您的應用程式架構。
2. 從版本 1.3 開始，relatedEvents 欄位為空白。您可以存取 LookupEvents API 參考中的AWS CloudTrail API，以擷取資源的事件。
3. 從版本 1.3 開始，configurationItemMD5Hash 欄位為空白。您可以使用 configurationStateId 欄位來確保您擁有最新的組態項目。

# 將組態快照交付到 Amazon S3 儲存貯體

AWS Config 將記錄 AWS 資源的 AWS Config 組態快照交付到您在設定交付通道時指定的 Amazon S3 儲存貯體。

主題


- 提供組態快照
- 範例組態快照來源 AWS Config

- 驗證交付狀態
- 檢視 Amazon S3 儲存貯體中的組態快照

## 提供組態快照

AWS Config 當您呼叫「快照」動作或執行 AWS CLI `deliver-config-snapshot`指令時，會產生組態DeliverConfig快照。 AWS Config 將組態快照存放在啟用時指定的 Amazon S3 儲存貯體中 AWS Config。

透過`deliver-config-snapshot`指定設定傳送通道 AWS Config 時所指派的名稱來輸入命令，例如：

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

## 範例組態快照來源 AWS Config

以下是組態快照集中 AWS Config 包含的資訊範例。快照說明目前區域中記錄您 AWS Config 的資源的組態 AWS 帳戶，並說明這些資源之間的關係。

> **Note**
>
> 組態快照可以包含不受支援資源類型和資源 ID 的參考。

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
```

```
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
```

```
        {
            "configurationItemVersion": "1.0",
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
```

```
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
```

```
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
```

```
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

下一步是驗證已將組態快照成功交付至交付管道。

## 驗證交付狀態

輸入describe-delivery-channel-status命令以確認是否 AWS Config 已開始將組態傳遞至指定的傳遞通道，例如：

```
$ aws configservice describe-delivery-channel-status
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
```

```
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

回應會列出三種傳遞格式的狀態，這三種傳遞格式會 AWS Config 用來將組態傳遞至您的儲存貯體和主題。

請查看 `configSnapshotDeliveryInfo` 中的 `lastSuccessfulTime` 欄位。時間應該符合您上次請求交付組態快照的時間。

> **Note**
>
> AWS Config 使用 UTC 格式（國際標準時間）來記錄時間。

## 檢視 Amazon S3 儲存貯體中的組態快照

1. 登入 AWS Management Console 並開啟 Amazon S3 主控台，網址為 https://console.aws.amazon.com/s3/。
2. 在 Amazon S3 主控台 所有儲存貯體 清單中，按一下 Amazon S3 儲存貯體的名稱。
3. 按一下儲存貯體中的巢狀資料夾，直到您看到 `ConfigSnapshot` 物件，而其快照 ID 符合命令所傳回的 ID。下載並開啟物件，以檢視組態快照。

   S3 儲存貯體也包含名為的空檔案`ConfigWritabilityCheckFile`。 AWS Config 建立此檔案以驗證服務是否可成功寫入 S3 儲存貯體。

# AWS Config 傳送至 Amazon SNS 主題的通知

> **Note**
>
> 您必須先設定組態記錄器和交付通道，才AWS Config能將通知傳送至 Amazon SNS 主題。如需詳細資訊，請參閱管理組態錄製程式和管理傳遞通道。

您可以設定 AWS Config，以將組態變更和通知串流至 Amazon SNS 主題。例如，更新資源時，您可以收到傳送至您電子郵件的通知，因此您可以檢視變更。AWS Config 根據您的資源評估您的自訂或受管規則時，您也可以收到通知。如需詳細資訊，請參閱中的記錄和監視AWS Config。

AWS Config 會傳送下列事件的通知：

- 資源的組態項目變更。
- 已交付您帳戶的資源組態歷史記錄。
- 已針對您的帳戶啟動和交付所記錄資源的組態快照。
- 資源的合規性狀態，以及它們是否符合您的規則。
- 已針對您的資源開始規則的評估。
- AWS Config 無法將通知交付至您的帳戶。

主題


- 範例組態項目變更通知
- 範例組態歷史記錄交付通知
- 範例組態快照交付已啟動通知
- 範例組態快照交付通知
- 範例合規性變更通知
- 範例規則評估已啟動通知
- 範例大型組態項目變更通知
- 範例交付失敗通知

# 範例組態項目變更通知

AWS Config 使用 Amazon SNS 向訂閱端點傳遞通知。這些通知提供組態快照和組態歷史記錄的傳遞狀態，並提供每個組態項目，這些設定項目會在記錄的 AWS 資源組態變更時 AWS Config 建立。AWS Config 還會傳送通知，顯示您的資源是否符合您的規則。如果您選擇透過電子郵件傳送通知，則可以根據電子郵件的主旨行和訊息本文以在電子郵件用戶端應用程式中使用篩選條件。

下列 Amazon SNS 通知承載範例是在 AWS Config 偵測到 Amazon Elastic Block Store 磁碟區 `vol-ce676ccc` 連接至 ID 為 `i-344c463d` 的執行個體時所產生。通知包含資源的組態項目變更。

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "accountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
```

```
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
```

```
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```


## 含關係的資源組態項目

如果資源與其他資源相關，則變更該資源可能會產生多個組態項目。下列範例顯示如何為具有關係的資源 AWS Config 建立組態項目。

1. 您有 ID 為 `i-007d374c8912e3e90` 的 Amazon EC2 執行個體，而且執行個體與 Amazon EC2 安全群組 `sg-c8b141b4` 建立關聯。
2. 您更新 EC2 執行個體，以將安全群組變更為另一個安全群組 `sg-3f1fef43`。
3. 由於 EC2 執行個體與其他資源相關，因此 AWS Config 會建立多個組態項目，如下列範例所示：

此通知包含 EC2 執行個體在取代安全群組時的組態項目變更。


```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
```

```
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
```

```
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
```

```
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
```

```
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
                },
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
```

```
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
```

```
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
```

```
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


此通知包含與執行個體建立關聯之 EC2 安全群組 `sg-3f1fef43` 的組態項目變更。


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
```

```
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
```

```
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## 了解 Amazon SNS **ConfigurationItemChangeNotification** 通知中的 **configurationItemDiff** 欄位

AWS Config 每當資源的配置發生變化（創建/更新/刪除）時創建一個配置項目。如需 AWS Config 可記錄的受支援資源類型清單，請參閱支援的資源類型。 AWS Config 使用 Amazon SNS 在發生變更時傳送通知。Amazon SNS 通知承載包含欄位，可協助您追蹤指定 AWS 區域中的資源變更。

若要了解您收到 `ConfigurationItemChangeNotification` 通知的原因，請檢閱 `configurationItemDiff` 詳細資訊。這些欄位會根據變更類型而有所不同，並且可以形成不同的組合，例如「UPDATE-UPDATE」、「UPDATE-CREATE」和「DELETE-DELETE」。下列是部分常見組合的說明。

「UPDATE-CREATE」和「UPDATE-UPDATE」

下列範例包含資源直接關係與資源組態中的變更。`configurationItemDiff` 詳細資訊顯示了下列資訊：

已執行的動作：帳戶中存在的受管政策已附加至 AWS Identity and Access Management (IAM) 角色。

已執行的基本操作：UPDATE (更新帳號中資源類型 `AWS::IAM::Policy` 的關聯數量)。

變更類型組合：

1. 資源直接關係變更「UPDATE-CREATE」。在 IAM 政策和 IAM 角色之間建立了新的連接或關聯。
2. 資源組態變更「UPDATE-UPDATE」。當政策連接至 IAM 角色時，IAM 政策關聯的數量會從 2 增加到 3。

範例「UPDATE-CREATE」和「UPDATE-UPDATE」`configurationItemDiff` 通知：

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
```

```
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

下列範例包含資源直接關係與資源組態中的變更。`configurationItemDiff` 詳細資訊顯示了下列資訊：

已執行的動作：帳戶中存在的受管政策已與 IAM 使用者分離。

已執行的基本操作：UPDATE (更新與資源類型 `AWS::IAM::User` 相關聯的許可政策)。

變更類型組合：資源直接關係變更「UPDATE-DELETE」。帳戶中 IAM 使用者與 IAM 政策之間的關聯已刪除。

範例「UPDATE-DELETE」`configurationItemDiff` 通知：

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

DELETE-DELETE

下列範例包含資源直接關係與資源組態中的變更。`configurationItemDiff` 詳細資訊顯示了下列資訊：

已執行的動作：已刪除帳戶中存在的 IAM 角色。

已執行的基本操作：DELETE (已刪除資源類型 `AWS::IAM::Role` 的資源)。

變更類型組合：資源直接關係變更與資源組態變更「DELETE-DELETE」。刪除 IAM 角色的同時，也會刪除 IAM 政策與 IAM 角色之間的關聯。

範例「DELETE-DELETE」`configurationItemDiff` 通知：

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
```

```
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

## 範例組態歷史記錄交付通知

組態歷史記錄是資源類型在一般時間期間的組態項目集合。下列範例通知會在為您的帳號AWS Config傳送 CloudTrail 追蹤資源的組態歷程記錄時傳送。

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
```

```
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


## 範例組態快照交付已啟動通知

下列範例通知是 AWS Config 在 AWS Config 開始交付您帳戶的組態快照時所傳送。


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
```

```
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


## 範例組態快照交付通知

組態快照是您帳戶中所有已記錄資源和其組態的組態項目集合。下列範例通知是 AWS Config 在交付您帳戶的組態快照時所傳送。


```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

## 範例合規性變更通知

AWS Config 根據自訂或受管規則評估您的資源時，AWS Config 會傳送通知，以顯示資源是否符合規則。

以下是 CloudTrail 追蹤資源符合`cloudtrail-enabled` 受管理規則的範例通知。

```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
```

```
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


## 示例：Config 配置項目更改 | 亞馬遜 EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
```

```
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
```

```
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

## 範例規則評估已啟動通知

AWS Config 在開始根據您的資源評估自訂或受管規則時會傳送通知。下列是 AWS Config 開始評估 `iam-password-policy` 受管規則時的範例通知。

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
```

```
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## 範例大型組態項目變更通知

AWS Config 偵測到資源的組態變更時，會傳送組態項目通知。如果通知超過 Amazon 簡單通知服務 (Amazon SNS) 允許的大小上限，則通知會包含組態項目的簡短摘要。您可以在`s3BucketLocation`欄位中指定的 Amazon S3 儲存貯體位置檢視完整通知。

下列範例通知顯示 Amazon EC2 執行個體的組態項目。通知包括變更摘要，以及 Amazon S3 儲存貯體中通知的位置。

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
```

```
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/
us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

## 範例交付失敗通知

AWS Config如果AWS Config無法將組態快照或過大的組態項目變更通知傳送到 Amazon S3 儲存貯體，則傳送交付失敗通知。確認您已指定有效的 Amazon S3 儲存貯體。

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
```

```
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

# 管理及檢視 AWS 資源組態 AWS Config

AWS Config 可讓您評估、稽核和評估資 AWS 源的組態。

AWS 資源是您使用 AWS Command Line Interface (CLI) AWS Management Console、 AWS SDK 或 AWS 合作夥伴工具建立和管理的實體。 AWS 資源範例包括 Amazon EC2 執行個體、安全群組、Amazon VPC 和 Amazon 彈性區塊存放區。 AWS Config 指使用其唯一識別碼的每個資源，例如資源 ID 或 Amazon 資源名稱 (ARN)。

一些常見的用例包括：

- 雲端管理員：您可以追蹤和管理資源組態，以協助確保合規性、疑難排解問題，並保持對 AWS 環境的瞭解
- 安全分析師：您可以根據所需的狀態評估資源組態，以協助識別弱點並評估安全狀況。
- 合規主管：您可以持續稽核和監控資源組態，以協助確保遵守組織政策和產業標準。

主題


- 檢視 AWS Config 儀表板
- 支援的資源類型
- 依區域可用性列出的資源涵蓋範圍
- 錄製 AWS 資源
- 記錄第三方資源的組態
- 記錄受管執行個體的軟體組態
- 檢視 資源組態和歷史記錄
- 為您的 AWS Config 資源建立標籤


## 檢視 AWS Config 儀表板

使用儀表板查看資源、規則、一致性套件及其合規狀態的概觀，並以視覺化方式呈現 Amazon 的 AWS Config 用量和成功指標。 CloudWatch此頁面可協助您快速識別 AWS 帳戶中最常用的資源、符合性最低等級的符合性套件 AWS 帳戶、您的哪些規則或資源不相容 AWS 帳戶、哪些流量會推動您的 AWS Config 使用量，以及工作流程中發生的成功與失敗的關鍵指標。

使用 AWS Config 儀表板

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在左側導覽窗格中，請選擇 儀表板。

內容

- 合規性與資源庫存
- AWS Config 使用狀況和成功量度

## 合規性與資源庫存

設置完成後， AWS Config 開始記錄您指定的資源並根據您的規則對其進行評估。顯示您的資源、規則、一致性套件及其合規性狀態可能需 AWS Config 要幾分鐘的時間。

依合規分數的一致性套件

依合規分數的一致性套件 會顯示最多 10 個一致性分數最低的一致性套件。合規分數是在一致性套件中合規規則資源組合數目與一致性套件中可能規則資源組合總數的百分比。

此指標可提供一致性套件合規狀態的高階檢視，並可用來識別、調查及了解一致性套件中的合規層級。您可以使用合規分數來追蹤修復進度、執行不同要求集的比較，以及查看特定變更或部署對一致性套件的影響。

若要在詳細檢視中檢視一致性套件的部署狀態、合規分數、合規分數時間表及規則，請在 一致性套件 下選擇一致性套件的名稱。

合規狀態

合規狀態 會顯示合規與不合規規則的數量，以及合規與不合規的資源。資源會根據與其相關聯之規則的評估，被判定為合規或不合規。如果資源不符合規則的規格，則資源和規則會標記為不合規。

若要檢視不合規規則和資源的清單，請選擇 不合規規則 或 不合規資源。

依不合規資源的規則

依不合規資源的規則 會依資源數量遞減順序顯示最常見的不合規規則。請選擇規則以檢視該特定規則的詳細資訊、參數及範圍內的資源。

如需不合規規則的完整清單，請選擇 檢視所有不合規規則。

資源庫存

「資源庫存」會依資源數目遞減順序顯示記錄的資源總數，以及您中各資源型態的個數 AWS 帳戶。 AWS Config 若要開啟某個資源類型的所有資源，請選擇該資源類型以移至其 資源清查 頁面。

您可以使用下拉式清單來指出您要檢視的資源總計。依預設，它設定為「檢視全部」資源，但您可以將其變更為 AWS 資源、協力廠商資源或自訂資源。

> **Note**
>
> [儀表板] 上可能會出現 [使用組 Config 規則評估 AWS 資源組態] 訊息，原因如下：
>
> - 您尚未為 AWS Config 您的 AWS 帳戶. 您可以選擇 Add rule (新增規則)，前往 Rules (規則) 頁面。
> - AWS Config 仍在根據您的規則評估您的資源。您可以重新整理頁面，查看最新的評估結果。
> - AWS Config 根據您的規則評估您的資源，並且在範圍內找不到任何資源。您可以在 [設定] 頁面中指定 AWS Config 要記錄的資源。如需詳細資訊，請參閱 錄製 AWS 資源。

## AWS Config 使用狀況和成功量度

您可以在 AWS Config 主控台中使用 Amazon CloudWatch 儀表板，以視覺化方式呈現您的 AWS Config 用量和成功指標。

您可以針對每個儀表板執行下列事項：

- 調整儀表板時間範圍，以顯示過去 3 小時、1 天或 1 週的資料。
- 選擇「行事曆」圖示，以輸入自訂時間範圍：過去指定時間量的相對時間或兩個日期之間的絕對時間範圍。
- 您可以變更時間格式，以 UTC (國際標準時間) 或當地時區 (在裝置作業系統中指定為當地時區的時區) 顯示儀表板資料。
- 使用 重新整理圖示 旁的 下拉式箭頭，指定儀表板中資料的重新整理頻率，或關閉自動重新整理。選擇 關閉、10 秒、1 分鐘、2 分鐘、5 分鐘 或 15 分鐘，以變更重新整理間隔。
- 選擇 [其他選項] (垂直省略符號功能表)，將 AWS Config 使用狀況測量結果或您目前在 [ AWS Config 儀表板] 中檢視的 AWS Config 成功量度新增至 CloudWatch 主控台。這會在 CloudWatch

主控台中開啟新索引標籤，可讓您在中建立新的自訂儀表板，其中 CloudWatch 包含從目前 AWS Config 使用量度或 AWS Config 成功量度複製的資訊。

如果您想要使用執行這些量度的其他分析 CloudWatch，請在 CloudWatch 主控台左側導覽窗格中選擇「度量結果」，然後選擇「AWS/Config」。如需有關可從 CloudWatch 主控台執行動作的詳細資訊，請參閱使用CloudWatch 者指南中的使用 Amazon CloudWatch 儀表板和使用 Amazon 指 CloudWatch 標。

AWS Config 使用量測量

| 指標 | 描述 | 單位 | |
|---|---|---|---|
| `Configuration Items Recorded` | 針對每個資源類型或所有資源類型記錄的組態項目數目。配置項目代表支持 AWS 資源的各種屬性的 point-in-time 視圖。如需組態項目或所支援資源類型的詳細資訊，請參閱組態項目和支援的資源類型。 | 計數 | |

您可以使用下拉式清單選取要檢視的資源類型。其預設會設定為檢視所有資源類型。

AWS Config 成功度量

| 指標 | 描述 | 單位 | |
|---|---|---|---|
| `Change Notifications Delivery Failed` | 傳送至 Amazon SNS 主題的失敗變更通知交付數目。變更通知會通知您有關 AWS 資源組態狀態的變更。您可以使用 ConfigStreamDeliveryInfoAPI 取得變更通知上次嘗試傳送的`lastErrorCode` 或`lastErrorMessage` 。如需詳細資訊，請參閱《管理交付管道》。 | 計數 | |
| `Config History Export Failed` | 將失敗的組態歷史記錄匯出到 Amazon S3 儲存貯體的數量。組態歷史記錄是指定資源在特定期間的組態項目集合。如需組態歷史記錄的詳細資訊，請參閱組態歷史記錄。 | 計數 | |

| 指標 | 描述 | 單位 | |
|---|---|---|---|
| `Configuration Recorder Insufficient Permissions Failure` | 由於組態錄製程式的 IAM 角色政策權限不足而導致的權限存取嘗試失敗次數。組態記錄器可偵測資源組態中的變更，並將這些變更作為組態項目擷取。若要讓組態記錄程式記錄您的 AWS 資源設定，需要必要的 IAM 許可。如需詳細資訊，請參閱用於取得組態詳細資訊的 IAM 角色政策。 | 計數 | |
| `Config Snapshot Export Failed` | 將失敗的組態快照匯出到 Amazon S3 儲存貯體的數量。組態快照是帳戶中所支援資源的組態項目集合。如需組態快照的詳細資訊，請參閱組態快照。 | 計數 | |

# 支援的資源類型

> **Important**
>
> 此頁面會在每月開始按月節奏進行更新。

AWS Config 支援下列 AWS 資源類型和資源關係。

- 如需有關資源類型的詳細資訊，請參閱《 AWS CloudFormation 使用指南》中的AWS 資源和屬性類型參考資訊 (例如語法、屬性和傳回值)。
- 對於 AWS Config 錄製，某些 AWS 區域支持這些資源類型的子集。如需哪些區域支援哪些資源類型的資訊，請參閱《依區域可用性列出的資源涵蓋範圍》。
- 進階查詢支 AWS Config 援這些資源類型的子集。如需這類所支援資源類型的清單，請參閱《進階查詢支援的資源類型》。
- 主動評估支 AWS Config 援這些資源類型的子集。如需所支援資源類型的清單，請參閱《主動評估支援的資源類型》。
- 定期規則會在不啟用組態記錄器的情況下執行，因為定期規則非取決於組態項目。如需變更觸發規則與週期性規則之間差異的詳細資訊，請參閱規則的評估模式與觸發器類型。 AWS Config

> **Note**
>
> 在指定 AWS Config 要追蹤的資源型態之前，請先勾選「依可用區域的資源涵蓋範圍」，以查看您設定的「 AWS 區域」中是否支援資源型態 AWS Config。如果至少一個「區域」支援某個資源類型，則您可以 AWS Config 在所支援的所有「區域」中啟用該資源類型的記錄 AWS Config，即使您設定的「 AWS 區域」不支援指定的資源類型也一樣 AWS Config。

## Amazon AppStream

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon AppStream | `AWS::AppStream::DirectoryConfig` | NA | 不適用 |
| | `AWS::AppStream::Application` | 不適用 | 不適用 |
| | `AWS::AppStream::Stack` | 不適用 | 不適用 |
| | `AWS::AppStream::Fleet` | 不適用 | NA |

## Amazon AppFlow

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon AppFlow | `AWS::AppFlow::Flow` | NA | NA |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon AppIntegrations | `AWS::AppIntegrations::EventIntegration` | NA | NA |

## Amazon API Gateway

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| API Gateway | `AWS::ApiGateway::Stage` | 包含於 | ApiGateway 休息 API |
| | | 關聯至 | WAFRegional WebACL |
| | `AWS::ApiGateway::RestApi` | contains | ApiGateway 舞台 |
| API Gateway V2 | `AWS::ApiGatewayV2::Stage` | 包含於 | ApiGatewayAPI |
| | `AWS::ApiGatewayV2::Api` | contains | ApiGateway第二階段 |

若要進一步了解如何 AWS Config 與 Amazon API Gateway 整合，請參閱使用 AWS Config.

## Amazon Athena

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Athena | `AWS::Athena::WorkGroup` | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::Athena::DataCatalog` | 不適用 | 不適用 |
| | `AWS::Athena::PreparedStatement` | 不適用 | NA |

## Amazon CloudFront

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon CloudFront | `AWS::CloudFront::Distribution` | 關聯至 | AWS WAF WebACL |
| | | | ACM 憑證 |
| | | | S3 儲存貯體 |
| | | | IAM 伺服器憑證 |
| | `AWS::CloudFront::StreamingDistribution` | 關聯至 | AWS WAF WebACL |
| | | | ACM 憑證 |
| | | | S3 儲存貯體 |
| | | | IAM 伺服器憑證 |

## Amazon CloudWatch

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon CloudWatch | `AWS::CloudWatch::Alarm` | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::CloudWatch::MetricStream` | 不適用 | NA |
| Amazon CloudWatch 日誌 | `AWS::Logs::Destination` | NA | NA |
| Amazon CloudWatch 朗姆 | `AWS::RUM::AppMonitor` | NA | NA |
| Amazon CloudWatch 顯然 | `AWS::Evidently::Project` | NA | 不適用 |
| | `AWS::Evidently::Launch` | 不適用 | 不適用 |
| | `AWS::Evidently::Segment` | 不適用 | NA |

## Amazon CodeGuru

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon 評論 CodeGuru 家 | `AWS::CodeGuruReviewer::RepositoryAssociation` | NA | NA |
| Amazon CodeGuru 分析器 | `AWS::CodeGuruProfiler::ProfilingGroup` | NA | NA |

## Amazon Cognito

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Cognito | `AWS::Cognito::UserPool` | NA | 不適用 |
| | `AWS::Cognito::UserPoolClient` | 不適用 | 不適用 |
| | `AWS::Cognito::UserPoolGroup` | 不適用 | NA |

## Amazon Connect

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Connect | `AWS::Connect::PhoneNumber` | NA | 不適用 |
| | `AWS::Connect::QuickConnect` | 不適用 | 不適用 |
| | `AWS::Connect::Instance` | 不適用 | NA |
| Amazon Connect Customer Profiles | `AWS::CustomerProfiles::Domain` | NA | 不適用 |
| | `AWS::CustomerProfi` | 不適用 | NA |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `les::Objectype` | | |

## Amazon Detective

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Detective | `AWS::Detective::Graph` | NA | NA |

## Amazon DynamoDB

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon DynamoDB | `AWS::DynamoDB::Table` | NA | NA |

## Amazon Elastic Compute Cloud

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Elastic Compute Cloud | `AWS::EC2::Host` * | contains | EC2 執行個體 |
| | `AWS::EC2::EIP` | 連接至 | EC2 執行個體 |
| | | | 網路介面 |
| | `AWS::EC2::Instance` | contains | EC2 網路介面 |
| | | 關聯至 | EC2 安全群組 |
| | | 連接至 | Amazon EBS 磁碟區 |
| | | | EC2 彈性 IP (EIP) |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | | 包含於 | EC2 專用主機 |
| | | | 路由表 |
| | | | 子網路 |
| | | | 虛擬私有雲端 (VPC) |
| | AWS::EC2::NetworkInterface | 關聯至 | EC2 安全群組 |
| | | 連接至 | EC2 彈性 IP (EIP) |
| | | | EC2 執行個體 |
| | | 包含於 | 路由表 |
| | | | 子網路 |
| | | | 虛擬私有雲端 (VPC) |
| | AWS::EC2::SecurityGroup * | 關聯至 | EC2 執行個體 |
| | | | EC2 網路介面 |
| | | | 虛擬私有雲端 (VPC) |
| | AWS::EC2::NatGateway | 包含於 | 虛擬私有雲端 (VPC) |
| | | 包含於 | 子網路 |
| | AWS::EC2::EgressOnlyInternetGateway | 連接至 | 虛擬私有雲端 (VPC) |
| | AWS::EC2::EC2Fleet | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::EC2::SpotFleet | 不適用 | 不適用 |
| | AWS::EC2::PrefixList | 不適用 | 不適用 |
| | AWS::EC2::FlowLog | 不適用 | 不適用 |
| | AWS::EC2::TransitGateway | 不適用 | 不適用 |
| | AWS::EC2::TransitGatewayAttachment | 不適用 | 不適用 |
| | AWS::EC2::TransitGatewayRouteTable | 不適用 | NA |
| | AWS::EC2::VPCEndpoint | 包含於 | 虛擬私有雲端 (VPC) |
| | | 連接至 | 網路介面 |
| | | 包含於 | 子網路 |
| | | 包含於 | 路由表 |
| | AWS::EC2::VPCEndpointService | 關聯至 | ElasticLoad平衡 V2 LoadBalancer |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::EC2::VPCPeeringConnection | 關聯至 | 虛擬私有雲端 (VPC) |
| | AWS::EC2::RegisteredHAInstance | 關聯至 | EC2 執行個體 |
| | AWS::EC2::SubnetRouteTableAssociation | NA | 不適用 |
| | AWS::EC2::LaunchTemplate | 不適用 | 不適用 |
| | AWS::EC2::NetworkInsightsAccessScopeAnalysis | 不適用 | 不適用 |
| | AWS::EC2::TrafficMirrorTarget | 不適用 | 不適用 |
| | AWS::EC2::TrafficMirrorSession | 不適用 | 不適用 |
| | AWS::EC2::DHCPOptions | 不適用 | 不適用 |
| | AWS::EC2::IPAM | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::EC2::NetworkInsightsPath | 不適用 | 不適用 |
| | AWS::EC2::TrafficMirrorFilter | 不適用 | 不適用 |
| | AWS::EC2::CapacityReservation | 不適用 | 不適用 |
| | AWS::EC2::ClientVpnEndpoint | 不適用 | NA |
| | AWS::EC2::CustomerGateway | 連接至 | VPN 連接 |
| | AWS::EC2::InternetGateway | 連接至 | 虛擬私有雲端 (VPC) |
| | AWS::EC2::NetworkAcl | NA | NA |
| | AWS::EC2::RouteTable | contains | EC2 執行個體 |
| | | | EC2 網路介面 |
| | | | 子網路 |
| | | | VPN 閘道 |
| | | 包含於 | 虛擬私有雲端 (VPC) |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::EC2::Subnet | contains | EC2 執行個體 |
| | | | EC2 網路介面 |
| | | 連接至 | 網路 ACL |
| | | 包含於 | 路由表 |
| | | | 虛擬私有雲端 (VPC) |
| | AWS::EC2::VPC | contains | EC2 執行個體 |
| | | | EC2 網路介面 |
| | | | 網路 ACL |
| | | | 路由表 |
| | | | 子網路 |
| | | 關聯至 | 安全群組 |
| | | 連接至 | 網際網路閘道 |
| | | | VPN 閘道 |
| | AWS::EC2::VPNConnection | 連接至 | 客戶閘道 |
| | | | VPN 閘道 |
| | AWS::EC2::VPNGateway | 連接至 | 虛擬私有雲端 (VPC) |
| | | | VPN 連接 |
| | | 包含於 | 路由表 |
| | AWS::EC2::IPAMScope | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::EC2::CarrierGateway | 不適用 | 不適用 |
| | AWS::EC2::TransitGatewayConnect | 不適用 | 不適用 |
| | AWS::EC2::IPAMPool | 不適用 | 不適用 |
| | AWS::EC2::TransitGatewayMulticastDomain | 不適用 | 不適用 |
| | AWS::EC2::NetworkInsightsAccessScope | 不適用 | 不適用 |
| | AWS::EC2::NetworkInsightsAnalysis | 不適用 | NA |
| Amazon Elastic Block Store | AWS::EC2::Volume | 連接至 | EC2 執行個體 |
| EC2 Image Builder | AWS::ImageBuilder::ImagePipeline | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::ImageBuilder::DistributionConfiguration | 不適用 | 不適用 |
| | AWS::ImageBuilder::ContainerRecipe | 不適用 | 不適用 |
| | AWS::ImageBuilder::InfrastructureConfiguration | 不適用 | 不適用 |
| | AWS::ImageBuilder::ImageRecipe | 不適用 | NA |

*AWS Config 記錄專用主機的組態詳細資料，以及您在其上啟動的執行個體。因此，當您報告符合伺服器繫結軟體授權時，您可以用 AWS Config 作資料來源。例如，您可以檢視執行個體的組態歷史記錄，並判斷它是以哪個 Amazon Machine Image (AMI) 為基礎。然後，您可以查詢主機的組態歷史記錄，其中包含詳細資訊 (例如通訊端和核心數目)，以檢查主機是否符合 AMI 的授權要求。如需詳細資訊，請參閱 Amazon EC2 使用者指南 AWS Config中的使用追蹤組態變更。

* EC2 SecurityGroup 屬性定義包含 IP CIDR 區塊，這些區塊會在內部轉換為 IP 範圍，而且在嘗試尋找特定 IP 範圍時可能會傳回未預期的結果。如需搜尋特定 IP 範圍的因應措施，請參閱《進階查詢的限制》。

## Amazon Elastic Container Registry

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Elastic Container Registry | `AWS::ECR::Repository` | NA | 不適用 |
| | `AWS::ECR::RegistryPolicy` | 不適用 | 不適用 |
| | `AWS::ECR::PullThroughCacheRule` | 不適用 | NA |
| Amazon Elastic Container Registry Public | `AWS::ECR::PublicRepository` | NA | NA |

## Amazon Elastic Container Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Elastic Container Service | `AWS::ECS::Cluster` | NA | 不適用 |
| | `AWS::ECS::TaskDefinition` | 不適用 | 不適用 |
| | `AWS::ECS::Service` * | 不適用 | 不適用 |
| | `AWS::ECS::TaskSet` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::ECS::Capacity Provider` | 不適用 | NA |

*此服務目前僅支援新的 Amazon Resource Name (ARN) 格式。如需詳細資訊，請參閱《ECS 開發人員指南》中的 Amazon Resource Name (ARN) 和 ID。

舊版 (不支援)：`arn:aws:ecs:region:aws_account_id:service/service-name`

新版 (支援)：`arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

## Amazon Elastic File System

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Elastic File System | `AWS::EFS::FileSystem` | NA | 不適用 |
| | `AWS::EFS::AccessPoint` | 不適用 | NA |

## Amazon Elastic Kubernetes Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Elastic Kubernetes Service | `AWS::EKS::Cluster` | NA | 不適用 |
| | `AWS::EKS::FargateProfile` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::EKS::IdentityProviderConfig` | 不適用 | 不適用 |
| | `AWS::EKS::Addon` | 不適用 | NA |

## Amazon EMR

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon EMR | `AWS::EMR::SecurityConfiguration` | NA | NA |

## Amazon EventBridge

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon EventBridge | `AWS::Events::EventBus` | NA | 不適用 |
| | `AWS::Events::ApiDestination` | 不適用 | 不適用 |
| | `AWS::Events::Archive` | 不適用 | 不適用 |
| | `AWS::Events::Endpoint` | 不適用 | 不適用 |
| | `AWS::Events::Connection` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::Events::Rule` | 不適用 | NA |
| Amazon EventBridge 模式 | `AWS::EventSchemas::RegistryPolicy` | NA | 不適用 |
| | `AWS::EventSchemas::Discoverer` | 不適用 | 不適用 |
| | `AWS::EventSchemas::Schema` | 不適用 | NA |

## Amazon Forecast

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Forecast | `AWS::Forecast::Dataset` | NA | 不適用 |
| | `AWS::Forecast::DatasetGroup` | 不適用 | NA |

## Amazon Fraud Detector

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Fraud Detector | `AWS::FraudDetector::Label` | NA | 不適用 |
| | `AWS::FraudDetector::EntityType` | 不適用 | 不適用 |
| | `AWS::FraudDetector::Variable` | 不適用 | 不適用 |
| | `AWS::FraudDetector::Outcome` | 不適用 | NA |

## Amazon GuardDuty

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon GuardDuty | `AWS::GuardDuty::Detector` | NA | 不適用 |
| | `AWS::GuardDuty::ThreatIntelSet` | 不適用 | 不適用 |
| | `AWS::GuardDuty::IPSet` | 不適用 | 不適用 |
| | `AWS::GuardDuty::Filter` | 不適用 | NA |

## Amazon Inspector

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Inspector | `AWS::InspectorV2::Filter` | NA | NA |

## Amazon Interactive Video Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Interactive Video Service | `AWS::IVS::Channel` | NA | 不適用 |
| | `AWS::IVS::RecordingConfiguration` | 不適用 | 不適用 |
| | `AWS::IVS::PlaybackKeyPair` | 不適用 | NA |

## Amazon Keyspaces (適用於 Apache Cassandra)

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Keyspaces (適用於 Apache Cassandra) | `AWS::Cassandra::Keyspace` | NA | NA |

## Amazon OpenSearch 服務

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon OpenSearch 服務 | `AWS::Elasticsearch::Domain` | 關聯至 | KMS 金鑰 |
| | | | EC2 安全群組 |
| | | | EC2 子網路 |
| | | | 虛擬私有雲端 (VPC) |
| | `AWS::OpenSearch::Domain` | NA | NA |

> **Note**
>
> 2021 年 9 月 8 日，Amazon Elasticsearch Service 更名為 Amazon OpenSearch 服務。OpenSearch 服務支持 OpenSearch 以及傳統的彈性搜索 OSS。如需詳細資訊，請參閱 Amazon OpenSearch 服務-變更摘要。
> 即使您將一個或多個網域升級到，您仍可以持續`AWS::OpenSearch::Domain`在現有`AWS::Elasticsearch::Domain`資源類型下看到您的資料數週 OpenSearch。

## Amazon Personalize

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Personalize | `AWS::Personalize::Dataset` | NA | 不適用 |
| | `AWS::Personalize::Schema` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::Personalize::Solution` | 不適用 | 不適用 |
| | `AWS::Personalize::DatasetGroup` | 不適用 | NA |

## Amazon Pinpoint

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Pinpoint | `AWS::Pinpoint::ApplicationSettings` | NA | 不適用 |
| | `AWS::Pinpoint::Segment` | 不適用 | 不適用 |
| | `AWS::Pinpoint::App` | 不適用 | 不適用 |
| | `AWS::Pinpoint::Campaign` | 不適用 | 不適用 |
| | `AWS::Pinpoint::InAppTemplate` | 不適用 | 不適用 |
| | `AWS::Pinpoint::EmailChannel` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::Pinpoint::EmailTemplate` | 不適用 | 不適用 |
| | `AWS::Pinpoint::EventStream` | 不適用 | NA |

## Amazon Quantum Ledger Database (Amazon QLDB)

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon QLDB | `AWS::QLDB::Ledger` | NA | NA |

## Amazon Kendra

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Kendra | `AWS::Kendra::Index` | NA | NA |

## Amazon Kinesis

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Kinesis | `AWS::Kinesis::Stream` | NA | 不適用 |
| | `AWS::Kinesis::StreamConsumer` | 不適用 | NA |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Kinesis Analytics V2 | `AWS::KinesisAnalyticsV2::Application` | NA | NA |
| Amazon 數據 Firehose | `AWS::KinesisFirehose::DeliveryStream` | NA | NA |
| Kinesis 視訊串流 | `AWS::KinesisVideo::SignalingChannel` | NA | 不適用 |
| | `AWS::KinesisVideo::Stream` | 不適用 | NA |

## Amazon Lex

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Lex | `AWS::Lex::BotAlias` | NA | 不適用 |
| | `AWS::Lex::Bot` | 不適用 | NA |

## Amazon Lightsail

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Lightsail | `AWS::Lightsail::Disk` | NA | 不適用 |
| | `AWS::Lightsail::Certificate` | 不適用 | 不適用 |
| | `AWS::Lightsail::Bucket` | 不適用 | 不適用 |
| | `AWS::Lightsail::StaticIp` | 不適用 | NA |

## Amazon Lookout for Metrics

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Lookout for Metrics | `AWS::LookoutMetrics::Alert` | NA | NA |

## Amazon Lookout for Vision

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Lookout for Vision | `AWS::LookoutVision::Project` | NA | NA |

## Amazon Managed Grafana

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Managed Grafana | `AWS::Grafana::Workspace` | NA | NA |

## Amazon Managed Service for Prometheus

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Managed Service for Prometheus | `AWS::APS::RuleGroupsNamespace` | NA | NA |

## Amazon MemoryDB for Redis

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon MemoryDB for Redis | `AWS::MemoryDB::SubnetGroup` | NA | NA |

## Amazon MQ

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon MQ | `AWS::AmazonMQ::Broker` | NA | NA |

## Amazon Managed Streaming for Apache Kafka

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Managed Streaming for Apache Kafka | `AWS::MSK::Cluster` | NA | 不適用 |
| | `AWS::MSK::Configuration` | 不適用 | 不適用 |
| | `AWS::MSK::BatchScramSecret` | 不適用 | 不適用 |
| | `AWS::MSK::ClusterPolicy` | 不適用 | 不適用 |
| | `AWS::MSK::VpcConnection` | 不適用 | NA |
| Amazon Managed Streaming for Apache Kafka Connect | `AWS::KafkaConnect::Connector` | NA | NA |

## Amazon Redshift

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Redshift | `AWS::Redshift::Cluster` | 關聯至 | 叢集參數群組 |
| | | | 叢集安全群組 |
| | | | 叢集子網路群組 |
| | | | 安全群組 |
| | | | 虛擬私有雲端 (VPC) |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::Redshift::ClusterParameterGroup | NA | 不適用 |
| | AWS::Redshift::ClusterSecurityGroup | 不適用 | 不適用 |
| | AWS::Redshift::ScheduledAction | 不適用 | NA |
| | AWS::Redshift::ClusterSnapshot | 關聯至 | 叢集 |
| | | | 虛擬私有雲端 (VPC) |
| | AWS::Redshift::ClusterSubnetGroup | 關聯至 | 子網路 |
| | | | 虛擬私有雲端 (VPC) |
| | AWS::Redshift::EventSubscription | NA | 不適用 |
| | AWS::Redshift::EndpointAccess | 不適用 | 不適用 |
| | AWS::Redshift::EndpointAuthorization | 不適用 | NA |

# Amazon Relational Database Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Relational Database Service | `AWS::RDS::DBInstance` | 關聯至 | EC2 安全群組 |
| | | | RDS 資料庫安全群組 |
| | | | RDS 資料庫子網路群組 |
| | `AWS::RDS::DBSecurityGroup` | 關聯至 | EC2 安全群組 |
| | | | 虛擬私有雲端 (VPC) |
| | `AWS::RDS::DBSnapshot` | 關聯至 | 虛擬私有雲端 (VPC) |
| | `AWS::RDS::DBSubnetGroup` | 關聯至 | EC2 安全群組 |
| | | | 虛擬私有雲端 (VPC) |
| | `AWS::RDS::EventSubscription` | NA | NA |
| | `AWS::RDS::DBCluster` | contains | RDS 資料庫執行個體 |
| | | 關聯至 | RDS 資料庫子網路群組 |
| | | | EC2 安全群組 |
| | `AWS::RDS::DBClusterSnapshot` | 關聯至 | RDS 資料庫叢集 |
| | | | 虛擬私有雲端 (VPC) |
| | `AWS::RDS::GlobalCluster` | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::RDS::OptionGroup | 不適用 | NA |

## Amazon Route 53

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Route 53 | AWS::Route53::HostedZone | NA | 不適用 |
| | AWS::Route53::HealthCheck | 不適用 | 不適用 |
| Amazon Route 53 Resolver | AWS::Route53Resolver::ResolverEndpoint | 不適用 | 不適用 |
| | AWS::Route53Resolver::ResolverRule | 不適用 | 不適用 |
| | AWS::Route53Resolver::ResolverRuleAssociation | 不適用 | 不適用 |
| | AWS::Route53Resolver::FirewallDomainList | 不適用 | 不適用 |
| | AWS::Route53Resolver::FirewallRuleGroupAssociation | 不適用 | 不適用 |
| | AWS::Route53Resolver::ResolverQueryLoggingConfig | 不適用 | 不適用 |
| | AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | 不適用 | 不適用 |
| | AWS::Route53Resolver::FirewallRuleGroup | 不適用 | NA |
| Amazon Route 53 Applicati | AWS::Route53RecoveryReadiness::Cell | NA | 不適用 |
| | AWS::Route53RecoveryReadiness::ReadinessCheck | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| on Recovery Controller | AWS::Route53RecoveryReadiness::RecoveryGroup | 不適用 | 不適用 |
| | AWS::Route53RecoveryControl::Cluster | 不適用 | 不適用 |
| | AWS::Route53RecoveryControl::ControlPanel | 不適用 | 不適用 |
| | AWS::Route53RecoveryControl::RoutingControl | 不適用 | 不適用 |
| | AWS::Route53RecoveryControl::SafetyRule | 不適用 | 不適用 |
| | AWS::Route53RecoveryReadiness::ResourceSet | 不適用 | NA |

## Amazon SageMaker

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon SageMaker | AWS::SageMaker::CodeRepository | NA | 不適用 |
| | AWS::SageMaker::Domain | 不適用 | 不適用 |
| | AWS::SageMaker::AppImageConfig | 不適用 | 不適用 |
| | AWS::SageMaker::Image | 不適用 | 不適用 |
| | AWS::SageMaker::Model | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::SageMaker::NotebookInstance` | 不適用 | 不適用 |
| | `AWS::SageMaker::NotebookInstanceLifecycleConfig` | 不適用 | 不適用 |
| | `AWS::SageMaker::EndpointConfig` | 不適用 | 不適用 |
| | `AWS::SageMaker::Workteam` | 不適用 | 不適用 |
| | `AWS::SageMaker::FeatureGroup` | 不適用 | NA |

## Amazon Simple Email Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Simple Email Service | `AWS::SES::ConfigurationSet` | NA | 不適用 |
| | `AWS::SES::ContactList` | 不適用 | 不適用 |
| | `AWS::SES::Template` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::SES::ReceiptFilter` | 不適用 | 不適用 |
| | `AWS::SES::ReceiptRuleSet` | 不適用 | NA |

## Amazon Simple Notification Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Simple Notification Service | `AWS::SNS::Topic` | NA | NA |

## Amazon Simple Queue Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Simple Queue Service | `AWS::SQS::Queue` | NA | NA |

## Amazon Simple Storage Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon Simple Storage Service | `AWS::S3::Bucket` * | NA | 不適用 |
| | `AWS::S3::AccountPublicAccessBlock` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::S3::MultiRegionAccessPoint` | 不適用 | 不適用 |
| | `AWS::S3::StorageLens` | 不適用 | 不適用 |
| | `AWS::S3::AccessPoint` | 不適用 | NA |

* 如果您設定 AWS Config 為記錄 S3 儲存貯體，但未收到組態變更通知，請檢查 S3 儲存貯體政策是否具有必要的許可。如需詳細資訊，請參閱 管理 S3 儲存貯體記錄的許可。

Amazon S3 儲存貯體屬性

AWS Config 也會記錄下列 Amazon S3 儲存貯體資源類型的屬性。

| Attributes | 描述 |
| --- | --- |
| AccelerateConfiguration | 加速用戶端與儲存貯體之間長距離的資料傳輸。 |
| BucketAcl | 存取控制清單用來管理儲存貯體和物件的存取。 |
| BucketPolicy | 政策定義儲存貯體的許可。 |
| CrossOrigin配置 | 允許儲存貯體的跨來源請求。 |
| LifecycleConfiguration | 規則定義儲存貯體中物件的生命週期。 |
| LoggingConfiguration | 記錄日誌用來追蹤存取儲存貯體的請求。 |
| NotificationConfiguration | 事件通知用來針對指定的儲存貯體事件傳送提醒或觸發工作流程。 |
| ReplicationConfiguration | 將物件自動非同步複製至不同 AWS 區域中的儲存貯體。 |
| RequestPayment配置 | 啟用申請者付款。 |

| Attributes | 描述 |
| --- | --- |
| TaggingConfiguration | 新增至儲存貯體以進行分類的標籤。您也可以使用標記來追蹤計費。 |
| WebsiteConfiguration | 啟用儲存貯體的靜態網站託管。 |
| VersioningConfiguration | 啟用儲存貯體中物件的版本控制。 |

如需屬性的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的儲存貯體組態選項。

## Amazon WorkSpaces

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Amazon WorkSpaces | `AWS::WorkSpaces::ConnectionAlias` | NA | 不適用 |
| | `AWS::WorkSpaces::Workspace` | 不適用 | NA |

## AWS Amplify

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Amplify | `AWS::Amplify::App` | NA | 不適用 |
| | `AWS::Amplify::Branch` | 不適用 | NA |

# AWS AppConfig

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS AppConfig | `AWS::AppConfig::Application` | NA | 不適用 |
| | `AWS::AppConfig::Environment` | 不適用 | 不適用 |
| | `AWS::AppConfig::ConfigurationProfile` | 不適用 | 不適用 |
| | `AWS::AppConfig::DeploymentStrategy` | 不適用 | 不適用 |
| | `AWS::AppConfig::HostedConfigurationVersion` | 不適用 | 不適用 |
| | `AWS::AppConfig::ExtensionAssociation` | 不適用 | NA |

## AWS App Runner

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS App Runner | `AWS::AppRunner::VpcConnector` | NA | 不適用 |
| | `AWS::AppRunner::Service` | 不適用 | NA |

## AWS App Mesh

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS App Mesh | `AWS::AppMesh::VirtualNode` | NA | 不適用 |
| | `AWS::AppMesh::VirtualService` | 不適用 | 不適用 |
| | `AWS::AppMesh::VirtualGateway` | 不適用 | 不適用 |
| | `AWS::AppMesh::VirtualRouter` | 不適用 | 不適用 |
| | `AWS::AppMesh::Route` | 不適用 | 不適用 |
| | `AWS::AppMesh::GatewayRoute` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::AppMesh::Mesh` | 不適用 | NA |

## AWS AppSync

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS AppSync | `AWS::AppSync::GraphQLApi` | NA | NA |

## AWS Audit Manager

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Audit Manager | `AWS::AuditManager::Assessment` | NA | NA |

## AWS Auto Scaling

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Auto Scaling | `AWS::AutoScaling::AutoScalingGroup` | contains | Amazon EC2 執行個體 |
| | | 關聯至 | Classic Load Balancer |
| | | | Auto Scaling 啟動組態 |
| | | | 子網路 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::AutoScaling::LaunchConfiguration` | 關聯至 | Amazon EC2 安全群組 |
| | `AWS::AutoScaling::ScalingPolicy` | 關聯至 | Auto Scaling 群組 |
| | | | 警示 |
| | `AWS::AutoScaling::ScheduledAction` | 關聯至 | Auto Scaling 群組 |
| | `AWS::AutoScaling::WarmPool` | NA | NA |

## AWS Backup

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Backup | `AWS::Backup::BackupPlan` | NA | NA* |
| | `AWS::Backup::BackupSelection` | NA | 不適用 |
| | `AWS::Backup::BackupVault` | NA | NA* |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::Backup::RecoveryPoint` | NA | 不適用 |
| | `AWS::Backup::ReportPlan` | 不適用 | NA |

由於 AWS Backup 運作方式，其中一些資源類型與此表格中的其他 AWS Backup 資源類型有關。

`AWS::Backup::BackupPlan`與「Backup 計畫」有多個選項的`AWS::Backup::BackupSelection`位`AWS::Backup::RecoveryPoint`置相關，`AWS::Backup::BackupVault`且與 AWS Backup Vault 具有多個復原點的位置有關。

如需詳細資訊，請參閱《使用備份計畫管理備份》和《使用備份保存庫》。

## AWS Batch

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Batch | `AWS::Batch::JobQueue` | NA | 不適用 |
| | `AWS::Batch::ComputeEnvironment` | 不適用 | 不適用 |
| | `AWS::Batch::SchedulingPolicy` | 不適用 | NA |

## AWS Budgets

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Budgets | `AWS::Budgets::BudgetsAction` | NA | NA |

## AWS Certificate Manager

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Certificate Manager | `AWS::ACM::Certificate` | NA | NA |

## AWS CloudFormation

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS CloudFormation | `AWS::CloudFormation::Stack` * | contains | 支援的 AWS 資源類型 |

* 將配置更改AWS Config 記錄到 AWS CloudFormation 堆棧中以及堆棧中支持的資源類型。 AWS Config 不會記錄堆疊中尚未支援之資源類型的組態變更。不支援的資源類型會出現在堆疊之組態項目的補充組態區段中。

## AWS CloudTrail

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS CloudTrail | `AWS::CloudTrail::Trail` | NA | NA |

## AWS Cloud9

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Cloud9 | `AWS::Cloud9::EnvironmentEC2` | NA | NA |

## AWS Cloud Map

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| 服務探索 | `AWS::ServiceDiscovery::Service` | NA | 不適用 |
| | `AWS::ServiceDiscovery::PublicDnsNamespace` | 不適用 | 不適用 |
| | `AWS::ServiceDiscovery::HttpNamespace` | 不適用 | 不適用 |
| `AWS::ServiceDiscovery::Instance` | 不適用 | NA | |

## AWS CodeArtifact

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS CodeArtifact | `AWS::CodeArtifact::Repository` | NA | NA |

## AWS CodeBuild

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS CodeBuild | `AWS::CodeBuild::Project` * | 關聯至 | S3 儲存貯體 |
| | | | IAM 角色 |
| | `AWS::CodeBuild::ReportGroup` | NA | NA |

* 若要深入瞭解如何與 AWS Config 整合 AWS CodeBuild，請參閱與AWS CodeBuild 範例 AWS Config 搭配使用。

## AWS CodeDeploy

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS CodeDeploy | `AWS::CodeDeploy::Application` | contains | DeploymentGroup |
| | `AWS::CodeDeploy::DeploymentConfig` | NA | NA |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::CodeDeploy::DeploymentGroup` | 包含於 | 應用程式 |

## AWS CodePipeline

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS CodePipeline | `AWS::CodePipeline::Pipeline` * | 連接至 | S3 儲存貯體 |
| | | 關聯至 | IAM 角色 |
| | | | 程式碼專案 |
| | | | Lambda 函數 |
| | | | Cloudformation 堆疊 |
| | | | ElasticBeanstalk 應用 |

*AWS Config 記錄管線中 CodePipeline 管道和支援資源類型的組態變更。 AWS Config 不會記錄管線中尚未支援之資源類型的組態變更。不支援的資源類型 (例如 `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, 和 `ECS service`) 會出現在堆疊之組態項目的補充組態區段中。

## AWS Config

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Config | `AWS::Config::ResourceCompliance` * | 關聯至 | 所有資源* |
| | `AWS::Config::Confo` | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | rmancePackCompliance | | |
| | AWS::Config::ConfigurationRecorder * | 不適用 | NA |

*AWS::Config::ResourceCompliance 與相關資源之間的關係，取決於該特定資源類型的 AWS::Config::ResourceCompliance 報告的合規性。

* AWS::Config::ConfigurationRecorder 是系統資源類型 AWS Config ，此資源類型的記錄預設為啟用。

> **Note**
>
> AWS::Config::ConformancePackCompliance 與 AWS::Config::ConfigurationRecorder 資源類型的記錄不收取額外費用。

## AWS Database Migration Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Database Migration Service | AWS::DMS::EventSubscription | NA | 不適用 |
| | AWS::DMS::ReplicationSubnetGroup | 不適用 | 不適用 |
| | AWS::DMS::ReplicationInstance | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::DMS::ReplicationTask | 不適用 | 不適用 |
| | AWS::DMS::Certificate | 不適用 | 不適用 |
| | AWS::DMS::Endpoint | 不適用 | NA |

## AWS DataSync

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS DataSync | AWS::DataSync::LocationSMB | NA | 不適用 |
| | AWS::DataSync::LocationFSxLustre | 不適用 | 不適用 |
| | AWS::DataSync::LocationFSxWindows | 不適用 | 不適用 |
| | AWS::DataSync::LocationS3 | 不適用 | 不適用 |
| | AWS::DataSync::LocationEFS | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::DataSync::LocationNFS | 不適用 | 不適用 |
| | AWS::DataSync::LocationHDFS | 不適用 | 不適用 |
| | AWS::DataSync::LocationObjectStorage | 不適用 | 不適用 |
| | AWS::DataSync::Task | 不適用 | NA |

## AWS Device Farm

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Device Farm | AWS::DeviceFarm::TestGridProject | NA | 不適用 |
| | AWS::DeviceFarm::InstanceProfile | 不適用 | 不適用 |
| | AWS::DeviceFarm::Project | 不適用 | NA |

## AWS Elastic Beanstalk

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Elastic Beanstalk | `AWS::ElasticBeanstalk::Application` | contains | Elastic Beanstalk 應用程式版本 |
| | | | Elastic Beanstalk 環境 |
| | | 關聯至 | IAM 角色 |
| | `AWS::ElasticBeanstalk::ApplicationVersion` | 包含於 | Elastic Beanstalk 應用程式 |
| | | 關聯至 | Elastic Beanstalk 環境 |
| | | | S3 儲存貯體 |
| | `AWS::ElasticBeanstalk::Environment` | 包含於 | Elastic Beanstalk 應用程式 |
| | | 關聯至 | Elastic Beanstalk 應用程式版本 |
| | | | IAM 角色 |
| | | contains | CloudFormation 堆疊 |

## AWS Fault Injection Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Fault Injection Service | `AWS::FIS::ExperimentTemplate` | NA | NA |

## AWS Global Accelerator

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Global Accelerator | `AWS::GlobalAccelerator::Listener` | NA | 不適用 |
| | `AWS::GlobalAccelerator::EndpointGroup` | 不適用 | 不適用 |
| | `AWS::GlobalAccelerator::Accelerator` | 不適用 | NA |

## AWS Glue

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Glue | `AWS::Glue::Job` | NA | 不適用 |
| | `AWS::Glue::Classifier` | 不適用 | 不適用 |
| | `AWS::Glue::MLTransform` | 不適用 | NA |

## AWS Ground Station

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Ground Station | `AWS::GroundStation::Config` | NA | 不適用 |
| | `AWS::GroundStation::MissionProfile` | 不適用 | 不適用 |
| | `AWS::GroundStation::DataflowEndpointGroup` | 不適用 | NA |

## AWS HealthLake

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS HealthLake | `AWS::HealthLake::FHIRDatastore` | NA | NA |

## AWS Identity and Access Management (IAM)

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Identity and Access Management | `AWS::IAM::User` | 連接至 | IAM 群組 |
| | | | IAM 客戶管理政策 |
| | `AWS::IAM::Group` | contains | IAM 使用者 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | | 連接至 | IAM 客戶管理政策 |
| | AWS::IAM::Role | 連接至 | IAM 客戶管理政策 |
| | AWS::IAM::Policy | 連接至 | IAM 使用者 |
| | | | IAM 群組 |
| | | | IAM 角色 |
| | AWS::IAM::SAMLProvider | NA | 不適用 |
| | AWS::IAM::ServerCertificate | 不適用 | 不適用 |
| | AWS::IAM::InstanceProfile | 不適用 | 不適用 |
| | AWS::IAM::OIDCProvider | 不適用 | 不適用 |
| AWS Identity and Access Management Access Analyzer | AWS::AccessAnalyzer::Analyzer | 不適用 | NA |

AWS Config 包含內嵌原則及其記錄的組態詳細資料。如需內嵌政策的詳細資訊，請參閱《IAM 使用者指南》中的受管政策和內嵌政策。

# AWS IoT

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS IoT | AWS::IoT::Authorizer | NA | 不適用 |
| | AWS::IoT::SecurityProfile | 不適用 | 不適用 |
| | AWS::IoT::RoleAlias | 不適用 | 不適用 |
| | AWS::IoT::Dimension | 不適用 | 不適用 |
| | AWS::IoT::Policy | 不適用 | 不適用 |
| | AWS::IoT::MitigationAction | 不適用 | 不適用 |
| | AWS::IoT::ScheduledAudit | 不適用 | 不適用 |
| | AWS::IoT::AccountAuditConfiguration | 不適用 | 不適用 |
| | AWS::IoTSiteWise::Gateway | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::IoT::CustomMetric | 不適用 | 不適用 |
| | AWS::IoT::JobTemplate | 不適用 | 不適用 |
| | AWS::IoT::ProvisioningTemplate | 不適用 | 不適用 |
| | AWS::IoT::CACertificate | 不適用 | 不適用 |
| AWS IoT Wireless | AWS::IoTWireless::ServiceProfile | 不適用 | 不適用 |
| | AWS::IoTWireless::MulticastGroup | 不適用 | 不適用 |
| | AWS::IoTWireless::FuotaTask | 不適用 | 不適用 |
| AWS IoT Core | AWS::IoT::FleetMetric | 不適用 | 不適用 |
| AWS IoT Analytics | AWS::IoTAnalytics::Datastore | 不適用 | 不適用 |
| | AWS::IoTAnalytics::Dataset | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | AWS::IoTAnalytics::Pipeline | 不適用 | 不適用 |
| | AWS::IoTAnalytics::Channel | 不適用 | 不適用 |
| AWS IoT Events | AWS::IoTEvents::Input | 不適用 | 不適用 |
| | AWS::IoTEvents::DetectorModel | 不適用 | 不適用 |
| | AWS::IoTEvents::AlarmModel | 不適用 | 不適用 |
| AWS IoT TwinMaker | AWS::IoTTwinMaker::Workspace | 不適用 | 不適用 |
| | AWS::IoTTwinMaker::Entity | 不適用 | 不適用 |
| | AWS::IoTTwinMaker::Scene | 不適用 | 不適用 |
| | AWS::IoTTwinMaker::SyncJob | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS IoT SiteWise | `AWS::IoTSiteWise::Dashboard` | 不適用 | 不適用 |
| | `AWS::IoTSiteWise::Project` | 不適用 | 不適用 |
| | `AWS::IoTSiteWise::Portal` | 不適用 | 不適用 |
| | `AWS::IoTSiteWise::AssetModel` | 不適用 | 不適用 |
| AWS IoT Greengrass Version 2 | `AWS::GreengrassV2::ComponentVersion` | 不適用 | NA |

## AWS Key Management Service

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Key Management Service | `AWS::KMS::Key` | NA | 不適用 |
| | `AWS::KMS::Alias` | 不適用 | NA |

## AWS Lambda

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Lambda | `AWS::Lambda::Function` | 關聯至 | IAM 角色 |
| | | | EC2 安全群組 |
| | | 包含於 | EC2 子網路 |
| | `AWS::Lambda::Alias` | NA | 不適用 |
| | `AWS::Lambda::CodeSigningConfig` | 不適用 | NA |

## AWS Mainframe Modernization

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Mainframe Modernization | `AWS::M2::Environment` | NA | NA |

## AWS Network Firewall

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Network Firewall | `AWS::NetworkFirewall::Firewall` | 連接至 | EC2 子網路 |
| | | 關聯至 | NetworkFirewall FirewallPolicy |
| | `AWS::NetworkFirewa` | 關聯至 | NetworkFirewall RuleGroup |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `ll::FirewallPolicy` | | |
| | `AWS::NetworkFirewall::RuleGroup` | NA | 不適用 |
| | `AWS::NetworkFirewall::TLSInspectionConfiguration` | 不適用 | NA |

## AWS Network Manager

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Network Manager | `AWS::NetworkManager::TransitGatewayRegistration` | NA | 不適用 |
| | `AWS::NetworkManager::Site` | 不適用 | 不適用 |
| | `AWS::NetworkManager::Device` | 不適用 | 不適用 |
| | `AWS::NetworkManager::Link` | 不適用 | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::NetworkManager::GlobalNetwork` | 不適用 | 不適用 |
| | `AWS::NetworkManager::CustomerGatewayAssociation` | 不適用 | 不適用 |
| | `AWS::NetworkManager::LinkAssociation` | 不適用 | 不適用 |
| | `AWS::NetworkManager::ConnectPeer` | 不適用 | NA |

## AWS Panorama

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Panorama | `AWS::Panorama::Package` | NA | NA |

## AWS Private Certificate Authority

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Private Certificate Authority | `AWS::ACMPCA::Certi` | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | ficateAuthority | | |
| | AWS::ACMPCA::CertificateAuthorityActivation | 不適用 | NA |

## AWS Resilience Hub

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Resilience Hub | AWS::ResilienceHub::ResiliencyPolicy | NA | 不適用 |
| | AWS::ResilienceHub::App | 不適用 | NA |

## AWS 資源總管

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS 資源總管 | AWS::ResourceExplorer2::Index | NA | NA |

## AWS RoboMaker

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS RoboMaker | `AWS::RoboMaker::RobotApplicationVersion` | NA | 不適用 |
| | `AWS::RoboMaker::RobotApplication` | 不適用 | 不適用 |
| | `AWS::RoboMaker::SimulationApplication` | 不適用 | NA |

## AWS Signer

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Signer | `AWS::Signer::SigningProfile` | NA | NA |

## AWS Secrets Manager

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Secrets Manager | `AWS::SecretsManager::Secret` | 關聯至 | Lambda 功能 |
| | | 關聯至 | KMS 金鑰 |

## AWS Service Catalog

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Service Catalog | `AWS::ServiceCatalog::CloudFormationProduct` | 包含於 | 產品組合 |
| | | 關聯至 | CloudFormationProvisionedProduct |
| | `AWS::ServiceCatalog::CloudFormationProvisionedProduct` | 關聯至 | 產品組合 |
| | | | CloudFormation产品 |
| | | | CloudFormation堆疊 |
| | `AWS::ServiceCatalog::Portfolio` | contains | CloudFormation产品 |

## AWS Shield

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Shield | `AWS::Shield::Protection` | 關聯至 | Amazon CloudFront 分佈 |
| | `AWS::ShieldRegional::Protection` | 關聯至 | EC2 EIP |
| | | 關聯至 | ElasticLoadBalancing 平衡器 |
| | | 關聯至 | ElasticLoad平衡 V2 LoadBalancer |

## AWS Step Functions

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Step Functions | `AWS::StepFunctions::Activity` | NA | 不適用 |
| | `AWS::StepFunctions::StateMachine` | 不適用 | NA |

## AWS Systems Manager

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Systems Manager | `AWS::SSM::ManagedInstanceInventory` * | 關聯至 | EC2 執行個體 |
| | `AWS::SSM::PatchCompliance` | 關聯至 | 受管執行個體清查 |
| | `AWS::SSM::AssociationCompliance` | 關聯至 | 受管執行個體清查 |
| | `AWS::SSM::FileData` | 關聯至 | 受管執行個體清查 |
| | `AWS::SSM::Document` | NA | NA |

*若要進一步了解受管執行個體清查，請參閱Recording Software Configuration for Managed Instances。

## AWS Transfer Family

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Transfer Family | AWS::Transfer::Agreement | NA | 不適用 |
| | AWS::Transfer::Connector | 不適用 | 不適用 |
| | AWS::Transfer::Workflow | 不適用 | 不適用 |
| | AWS::Transfer::Certificate | 不適用 | 不適用 |
| | AWS::Transfer::Profile | 不適用 | NA |

## AWS WAF

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS WAF | AWS::WAF::RateBasedRule | NA | 不適用 |
| | AWS::WAF::Rule | 不適用 | NA |
| | AWS::WAF::WebACL | 關聯至 | WAF 規則 |
| | | | WAF 速率規則 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | | | WAF Rulegroup |
| | AWS::WAF::RuleGroup | 關聯至 | WAF 規則 |
| | AWS::WAFRegional::RateBasedRule | NA | 不適用 |
| | AWS::WAFRegional::Rule | 不適用 | NA |
| | AWS::WAFRegional::WebACL | 關聯至 | ElasticLoad平衡 V2 LoadBalancer |
| | | | WAFRegional 規則 |
| | | | WAFRegional 速率規則 |
| | | | WAFRegional Rulegroup |
| | AWS::WAFRegional::RuleGroup | 關聯至 | WAFRegional 規則 |
| AWS WAF V2 | AWS::WAFv2::WebACL | 關聯至 | ElasticLoad平衡 V2 LoadBalancer |
| | | | ApiGateway 舞台 |
| | | | WAFv2 IPSet |
| | | | WAFV2 RegexPatternSet |
| | | | WAFV2 RuleGroup |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | | | WAFV2 ManagedRuleSet |
| | `AWS::WAFv2::RuleGroup` | 關聯至 | WAFv2 IPSet |
| | | | WAFV2 RegexPatternSet |
| | `AWS::WAFv2::ManagedRuleSet` | 關聯至 | WAFV2 RuleGroup |
| | `AWS::WAFv2::IPSet` | NA | 不適用 |
| | `AWS::WAFv2::RegexPatternSet` | 不適用 | NA |

## AWS X-Ray

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS X-Ray | `AWS::XRay::EncryptionConfig` | NA | NA |

## Elastic Load Balancing

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| Elastic Load Balancing | Application Load Balancer | 關聯至 | EC2 安全群組 |
| | | 連接至 | 子網路 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `AWS::ElasticLoadBalancingV2::LoadBalancer` | 包含於 | 虛擬私有雲端 (VPC) |
| | Application Load Balancer 接聽程式<br><br>`AWS::ElasticLoadBalancingV2::Listener` | NA | NA |
| | Classic Load Balancer<br><br>`AWS::ElasticLoadBalancing::LoadBalancer` | 關聯至 | EC2 安全群組 |
| | | 連接至 | 子網路 |
| | | 包含於 | 虛擬私有雲端 (VPC) |
| | Network Load Balancer<br><br>`AWS::ElasticLoadBalancingV2::LoadBalancer` | NA | NA |

## AWS Elemental MediaConnect

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Elemental MediaConnect | `AWS::MediaConnect:` | NA | 不適用 |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `:FlowEntitlement` | | |
| | `AWS::MediaConnect::FlowVpcInterface` | 不適用 | 不適用 |
| | `AWS::MediaConnect::FlowSource` | 不適用 | NA |

## AWS Elemental MediaPackage

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Elemental MediaPackage | `AWS::MediaPackage::PackagingGroup` | NA | 不適用 |
| | `AWS::MediaPackage::PackagingConfiguration` | 不適用 | NA |

## AWS Elemental MediaTailor

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| AWS Elemental MediaTailor | `AWS::MediaTailor::` | NA | NA |

| AWS 服務 | 資源類型值 | 關係 | 相關資源 |
| --- | --- | --- | --- |
| | `PlaybackConfiguration` | | |

# 依區域可用性列出的資源涵蓋範圍

## 北美洲和南美洲區域

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
| --- | --- | --- | --- | --- | --- | --- | --- |
| AWS::ACM::Certificate | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ACMPCA::CertificateAuthority | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ACMPCA::CertificateAuthority激活 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::APS::RuleGroups名稱區 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::AccessAnalyzer::Analyzer | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::AmazonMQ::Broker | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Amplify::App | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Amplify::Branch | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ApiGateway::RestApi | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ApiGateway::Stage | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ApiGatewayV2::Api | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ApiGatewayV2::Stage | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::AppConfig::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppConfig::ConfigurationProfile | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppConfig::DeploymentStrategy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppConfig::Environment | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppConfig::ExtensionAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppConfig::HostedConfiguration版本 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppFlow::Flow | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::AppIntegrations::EventIntegration | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::AppMesh::GatewayRoute | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppMesh::Mesh | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppMesh::Route | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppMesh::VirtualGateway | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppMesh::VirtualNode | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppMesh::VirtualRouter | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::AppMesh::VirtualService | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AppRunner::Service | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::AppRunner::VpcConnector | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::AppStream::Application | 是 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::AppStream::DirectoryConfig | 是 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::AppStream::Fleet | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::AppStream::Stack | 是 | 否 | 是 | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::AppSync::GraphQLapi | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Athena::DataCatalog | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Athena::PreparedStatement | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Athena::WorkGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::AuditManager::Assessment | 是 | 否 | 是 | 是 | 是 | 是 | 否 |
| AWS::AutoScaling::AutoScaling集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::LaunchConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::AutoScaling::ScalingPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::ScheduledAction | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::WarmPool | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Backup::BackupPlan | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Backup::BackupSelection | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Backup::BackupVault | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Backup::RecoveryPoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Backup::ReportPlan | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Batch::ComputeEnvironment | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Batch::JobQueue | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Batch::SchedulingPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Budgets::BudgetsAction | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::Cassandra::Keyspace | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Cloud9::EnvironmentEC2 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::CloudFormation::Stack | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::CloudFront::Distribution | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::CloudFront::StreamingDistribution | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::CloudTrail::Trail | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::CloudWatch::Alarm | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::CloudWatch::MetricStream | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::CodeArtifact::Repository | 是 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::CodeBuild::Project | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::CodeBuild::ReportGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::CodeDeploy::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::CodeDeploy::DeploymentConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::CodeDeploy::DeploymentGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::CodeGuruProfiler::ProfilingGroup | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::CodeGuruReviewer::RepositoryAssociation | 是 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::CodePipeline::Pipeline | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Cognito::UserPool | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Cognito::UserPool客戶端 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Cognito::UserPool集團 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Config::ConfigurationRecorder | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Config::ConformancePack合規 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Config::ResourceCompliance | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Connect::Instance | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Connect::PhoneNumber | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Connect::QuickConnect | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::CustomerProfiles::Domain | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::CustomerProfiles::ObjectType | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::DMS::Certificate | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DMS::Endpoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::DMS::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DMS::ReplicationInstance | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DMS::ReplicationSubnet集團 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DMS::ReplicationTask | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationEFS | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationF SxLustre | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationF SxWindows | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Data Sync::LocationHDFS | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationNFS | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::Loc ationObject儲存 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationS3 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::Loc ation中小企 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::DataSync::Task | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Detective::Graph | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::DeviceFarm::InstanceProfile | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::DeviceFarm::Project | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::DeviceFarm::TestGrid項目 | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::DynamoDB::Table | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Capacity Reservation | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::CarrierGateway | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::EC2::ClientVpn端點 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::EC2::CustomerGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::DHCPOptions | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::EC2Fleet | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::EIP | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::EgressOnlyInternetGateway | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::FlowLog | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::Host | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::EC2::IPAM | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::IPAMPool | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::IPAMScope | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::Instance | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::InternetGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::LaunchTemplate | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::NatGateway | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::EC2::NetworkAcl | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::NetworkInsightsAccessScope | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::NetworkInsightsAccessScope分析 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::NetworkInsights分析 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::NetworkInsights路徑 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::NetworkInterface | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::PrefixList | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::EC2::Registered哈實例 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::RouteTable | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SecurityGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SpotFleet | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::Subnet | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SubnetRouteTableAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::TrafficMirror過濾器 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::EC2::TrafficMirror階段 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::TrafficMirror目標 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGateway | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGateway附件 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGatewayConnect | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGatewayMulticastDomain | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGatewayRouteTable | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::EC2::VPC | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPCEndpoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: EC2:: VPC EndpointService | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: EC2:: VPC PeeringConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPNConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPNGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Volume | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::ECR::PublicRepository | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::ECR::PullThroughCacheRule | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ECR::RegistryPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ECR::Repository | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ECS::CapacityProvider | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ECS::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::Service | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::ECS::TaskDefinition | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::TaskSet | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EFS::AccessPoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EFS::FileSystem | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EKS::Addon | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EKS::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EKS::FargateProfile | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::EKS::Identity ProviderConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EMR::Security Configuration | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ElasticBeanstalk::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ElasticBeanstalk::ApplicationVersion | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ElasticBeanstalk::Environment | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ElasticLoadBalancing::LoadBalancer | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ElasticLoadBalancingV2::Listener | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::ElasticLoadBalancingV2::LoadBalancer | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Elasticsearch::Domain | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EventSchemas::Discoverer | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EventSchemas::Registry | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EventSchemas::RegistryPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::EventSchemas::Schema | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Events::ApiDestination | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Events::Archive | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Events::Connection | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Events::Endpoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Events::EventBus | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Events::Rule | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Evidently::Launch | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::Evidently::Project | 是 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Evidently::Segment | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::FIS::ExperimentTemplate | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Forecast::Dataset | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::Forecast::DatasetGroup | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::FraudDetector::EntityType | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::FraudDetector::Label | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::FraudDetector::Outcome | 是 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::FraudDetector::Variable | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::GlobalAccelerator::Accelerator | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::GlobalAccelerator::EndpointGroup | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::GlobalAccelerator::Listener | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Glue::Classifier | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Glue::Job | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Glue:: 毫升變換 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Grafana::Workspace | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::GreengrassV2::ComponentVersion | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::GroundStation::Config | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::GroundStation::DataflowEndpoint集團 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::GroundStation::MissionProfile | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::GuardDuty::Detector | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::GuardDuty::Filter | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Guard責任:: 集 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::GuardDuty::ThreatIntel套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Health湖:: F | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IAM::Group | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IAM::InstanceProfile | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::IAM::OIDCProvider | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::IAM::Policy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::IAM::Role | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IAM::SAMLProvider | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::IAM::ServerCertificate | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::IAM::User | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IVS::Channel | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IVS::PlaybackKey一對 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IVS::RecordingConfiguration | 否 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::ImageBuilder::ContainerRecipe | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ImageBuilder::DistributionConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ImageBuilder::ImagePipeline | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ImageBuilder::ImageRecipe | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ImageBuilder::InfrastructureConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::InspectorV2::Filter | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::AccountAudit配置 | 是 | 否 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::IoT::Authorizer | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT:: 緩存 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::CustomMetric | 是 | 否 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::Dimension | 是 | 否 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::FleetMetric | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::JobTemplate | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::MitigationAction | 是 | 否 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::IoT::Policy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::ProvisioningTemplate | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::RoleAlias | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::ScheduledAudit | 是 | 否 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoT::SecurityProfile | 是 | 否 | 是 | 是 | 是 | 是 | 否 |
| AWS::IoTAnalytics::Channel | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTAnalytics::Dataset | 是 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::IoTAnalytics::Datastore | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTAnalytics::Pipeline | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTEvents::AlarmModel | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::IoTEvents::DetectorModel | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::IoTEvents::Input | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::IoTSiteWise::AssetModel | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::IoTSiteWise::Dashboard | 是 | 否 | 是 | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::IoTSiteWise::Gateway | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::IoTSiteWise::Portal | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::IoTSiteWise::Project | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::IoTTwinMaker::ComponentType | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTTwinMaker::Entity | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTTwinMaker::Scene | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTTwinMaker::SyncJob | 否 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::IoTTwinMaker::Workspace | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTWireless::FuotaTask | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTWireless::MulticastGroup | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTWireless::ServiceProfile | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::KMS::Alias | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::KMS::Key | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::KafkaConnect::Connector | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Kendra::Index | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Kinesis::Stream | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Kinesis::StreamConsumer | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::KinesisAnalyticsV2::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::KinesisFirehose::DeliveryStream | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::KinesisVideo::SignalingChannel | 是 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::KinesisVideo::Stream | 是 | 是 | 是 | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Lambda::CodeSigningConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Lambda::Function | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Lex::Bot | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Lex::BotAlias | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Lightsail::Bucket | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Lightsail::Certificate | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Lightsail::Disk | 是 | 否 | 是 | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Lightsail::StaticIp | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Logs::Destination | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::LookoutMetrics::Alert | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::LookoutVision::Project | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::M2::Environment | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MSK::BatchScram秘密 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MSK::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::MSK::ClusterPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MSK::Configuration | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MSK::VpcConnection | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MediaConnect::FlowEntitlement | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MediaConnect::FlowSource | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MediaConnect::FlowVpc介面 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::MediaPackage::PackagingConfiguration | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::MediaPackage::PackagingGroup | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::MediaTailor::PlaybackConfiguration | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::MemoryDB::SubnetGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::NetworkFirewall::Firewall | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::NetworkFirewall::FirewallPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::NetworkFirewall::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Network防火牆:: TLS InspectionConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::NetworkManager::ConnectPeer | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::NetworkManager::CustomerGateway協會 | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::NetworkManager::Device | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::NetworkManager::GlobalNetwork | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::NetworkManager::Link | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::NetworkManager::LinkAssociation | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::NetworkManager::Site | 否 | 否 | 否 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::NetworkManager::TransitGateway注册 | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::OpenSearch::Domain | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Panorama::Package | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Personalize::Dataset | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Personalize::DatasetGroup | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Personalize::Schema | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Personalize::Solution | 是 | 否 | 是 | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Pinpoint::App | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Pinpoint::ApplicationSettings | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Pinpoint::Campaign | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Pinpoint::EmailChannel | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Pinpoint::EmailTemplate | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Pinpoint::EventStream | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::Pinpoint::InApp。模板 | 是 | 否 | 是 | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Pinpoint::Segment | 否 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::QLDB::Ledger | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::QuickSight::DataSource | 是 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::QuickSight::Template | 是 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::QuickSight::Theme | 是 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::RDS::DBCluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 ClusterSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::RDS::DBInstance | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SecurityGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::DBSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SubnetGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::GlobalCluster | 是 | 否 | 是 | 是 | 是 | 是 | 否 |
| AWS::RDS::OptionGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::RUM::AppMonitor | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::Redshift::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterParameter集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSecurity集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSubnet集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::EndpointAccess | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Redshift::EndpointAuthorization | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Redshift::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ScheduledAction | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ResilienceHub::App | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ResilienceHub::ResiliencyPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ResourceExplorer2::Index | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::RoboMaker::RobotApplication | 是 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::RoboMaker::RobotApplication版本 | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::RoboMaker::SimulationApplication | 是 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::Route53::HealthCheck | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::Route53::HostedZone | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::Route53RecoveryControl::Cluster | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Route53RecoveryControl::ControlPanel | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Route53RecoveryControl::RoutingControl | 否 | 否 | 否 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Route53RecoveryControl::SafetyRule | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Route53RecoveryReadiness::Cell | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Route53RecoveryReadiness::ReadinessCheck | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Route53RecoveryReadiness::RecoveryGroup | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Route53RecoveryReadiness::ResourceSet | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::Route53Resolver::FirewallDomain列表 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::FirewallRule集團 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Route53Resolver::FirewallRuleGroupAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::ResolverEndpoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig協會 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::ResolverRule | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::ResolverRule協會 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::S3::AccessPoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::S3::AccountPublicAccessBlock | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::S3::Bucket | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::S3::MultiRegionAccessPoint | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| AWS::S3::StorageLens | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SES::ConfigurationSet | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SES::ContactList | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SES::ReceiptFilter | 否 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::SES::ReceiptRule套裝 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::SES::Template | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SNS::Topic | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SQS::Queue | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SSM::AssociationCompliance | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SSM::Document | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SSM::FileData | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::SSM::ManagedInstance庫存 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SSM::PatchCompliance | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::AppImageConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::CodeRepository | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::Domain | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::EndpointConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::FeatureGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::SageMaker::Image | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::Model | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::NotebookInstance | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::SageMaker::Workteam | 是 | 否 | 是 | 是 | 否 | 是 | 否 |
| AWS::SecretsManager::Secret | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ServiceCatalog::CloudFormation产品 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ServiceCatalog::Portfolio | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ServiceDiscovery::HttpNamespace | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ServiceDiscovery::Instance | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ServiceDiscovery::PublicDns名稱區 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::ServiceDiscovery::Service | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Shield::Protection | 否 | 否 | 是 | 否 | 否 | 否 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::ShieldRegional::Protection | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Signer::SigningProfile | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::StepFunctions::Activity | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::StepFunctions::StateMachine | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Transfer::Agreement | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Transfer::Certificate | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Transfer::Connector | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::Transfer::Profile | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::Transfer::Workflow | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WAF::RateBased規則 | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::WAF::Rule | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::WAF::RuleGroup | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::WAF::WebACL | 否 | 否 | 是 | 否 | 否 | 否 | 否 |
| AWS::WAFRegional::RateBased規則 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::WAFRegional::Rule | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WAFRegional::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WAFRegional::WebACL | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WAFv2::IPSet | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WAFv2::ManagedRule套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WAFv2::RegexPattern套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WAFv2::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 美國西部 (加州北部) | 美國東部 (維吉尼亞北部) | 美國西部 (奧勒岡) | 美國東部 (俄亥俄) | 加拿大西部 (卡加利) | 加拿大 (中部) | 南美洲 (聖保羅) |
|---|---|---|---|---|---|---|---|
| AWS::WAFv2::WebACL | 是 | 是 | 是 | 是 | 是 | 是 | 否 |
| AWS::WorkSpaces::ConnectionAlias | 否 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::WorkSpaces::Workspace | 否 | 是 | 是 | 是 | 否 | 是 | 否 |
| AWS::XRay::EncryptionConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 |

## 歐洲區域

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::ACM::Certificate | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::ACMPCA::CertificateAuthority | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ACMPCA::CertificateAuthority激活 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::APS::RuleGroups名稱區 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::AccessAnalyzer::Analyzer | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AmazonMQ::Broker | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Amplify::App | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Amplify::Branch | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ApiGateway::RestApi | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::ApiGateway::Stage | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ApiGatewayV2::Api | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ApiGatewayV2::Stage | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AppConfig::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppConfig::ConfigurationProfile | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppConfig::DeploymentStrategy | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppConfig::Environment | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppConfig::ExtensionAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::AppConfig::HostedConfiguration版本 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppFlow::Flow | 否 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::AppIntegrations::EventIntegration | 否 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::AppMesh::GatewayRoute | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppMesh::Mesh | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppMesh::Route | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppMesh::VirtualGateway | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppMesh::VirtualNode | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::AppMesh::VirtualRouter | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppMesh::VirtualService | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AppRunner::Service | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::AppRunner::VpcConnector | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::AppStream::Application | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::AppStream::DirectoryConfig | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::AppStream::Fleet | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::AppStream::Stack | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::AppSync::GraphQLapi | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Athena::DataCatalog | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Athena::PreparedStatement | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Athena::WorkGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::AuditManager::Assessment | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::AutoScaling::AutoScaling集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::LaunchConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::ScalingPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::AutoScaling::ScheduledAction | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Auto Scaling::WarmPool | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Backup::BackupPlan | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Back up::BackupSelection | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Backup::BackupVault | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Back up::RecoveryPoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Backup::ReportPlan | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Batch::Comput eEnvironment | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Batch::JobQueue | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Batch::SchedulingPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Cassandra::Keyspace | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Cloud9::EnvironmentEC2 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::CloudFormation::Stack | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::CloudTrail::Trail | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::CloudWatch::Alarm | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::CloudWatch::MetricStream | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Code Artifact::Repository | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::CodeBuild::Project | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Code Build::ReportGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Code Deploy::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::CodeDeploy::D eploymentConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::CodeDeploy::D eploymentGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::CodeGuruProfi ler::ProfilingGroup | 是 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::CodeGuruRevie wer::RepositoryAssociation | 是 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::CodePipeline::Pipeline | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Cognito::UserPool | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Cognito::UserPool客戶端 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Cognito::UserPool集團 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Config::ConfigurationRecorder | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Config::ConformancePack合規 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Config::ResourceCompliance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Connect::Instance | 否 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Connect::PhoneNumber | 否 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::Connect::QuickConnect | 否 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::CustomerProfiles::Domain | 否 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::CustomerProfiles::ObjectType | 否 | 否 | 否 | 是 | 是 | 否 | 否 | 否 |
| AWS::DMS::Certificate | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DMS::Endpoint | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DMS::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DMS::ReplicationInstance | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::DMS::ReplicationSubnet集團 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DMS::ReplicationTask | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DataSync::LocationEFS | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::DataSync::LocationF SxLustre | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DataSync::LocationF SxWindows | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DataSync::LocationHDFS | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::DataSync::LocationNFS | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::DataSync::LocationObject儲存 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲(愛爾蘭) | 歐洲(法蘭克福) | 歐洲(倫敦) | 歐洲(巴黎) | 歐洲(斯德哥爾摩) | 歐洲(米蘭) | 歐洲(西班牙) | 歐洲(蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Data Sync::LocationS3 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::DataSync::Location中小企 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::DataSync::Task | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Detective::Graph | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::DynamoDB::Table | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Capacity Reservation | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::EC2::CarrierGateway | 否 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EC2::ClientVpn端點 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::CustomerGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::DHCPOptions | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::EC2Fleet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::EIP | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::EgressOnlyInternetGateway | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 |
| AWS::EC2::FlowLog | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 |
| AWS::EC2::Host | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::IPAM | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::IPAMPool | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::IPAMScope | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Instance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::InternetGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::LaunchTemplate | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::EC2::NatGateway | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 |
| AWS::EC2::NetworkAcl | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::NetworkInsightsAccessScope | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::NetworkInsightsAccessScope分析 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::EC2::NetworkInsights分析 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::EC2::NetworkInsights路徑 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::EC2::NetworkInterface | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::PrefixList | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Registered哈實例 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EC2::RouteTable | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SecurityGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::SpotFleet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Subnet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SubnetRouteTableAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::TrafficMirror過濾器 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EC2::TrafficMirror階段 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EC2::TrafficMirror目標 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EC2::TransitGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::TransitGateway附件 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::TransitGatewayConnect | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::EC2::TransitGatewayMulticastDomain | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::TransitGatewayRouteTable | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 |
| AWS::EC2::VPC | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPCEndpoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: EC2:: VPC EndpointService | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: EC2:: VPC PeeringConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPNConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::VPNGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Volume | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECR::PullThroughCacheRule | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECR::RegistryPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECR::Repository | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::CapacityProvider | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::Service | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::ECS::TaskDefinition | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::TaskSet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EFS::AccessPoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EFS::FileSystem | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EKS::Addon | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EKS::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EKS::FargateProfile | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EKS::Identity ProviderConfig | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EMR::Security Configuration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ElasticBeanstalk::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ElasticBeanstalk::ApplicationVersion | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ElasticBeanstalk::Environment | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ElasticLoadBalancing::LoadBalancer | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ElasticLoadBalancingV2::Listener | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ElasticLoadBalancingV2::LoadBalancer | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Elasticsearch::Domain | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::EventSchemas::Discoverer | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EventSchemas::Registry | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EventSchemas::RegistryPolicy | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::EventSchemas::Schema | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Events::ApiDestination | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Events::Archive | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Events::Connection | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Events::Endpoint | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Events::EventBus | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Events::Rule | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Evidently::Launch | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::Evidently::Project | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::Evidently::Segment | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::FIS::ExperimentTemplate | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Forecast::Dataset | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::Forecast::DatasetGroup | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::FraudDetector::EntityType | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::FraudDetector::Label | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::FraudDetector::Outcome | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::FraudDetector::Variable | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::Glue::Classifier | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Glue::Job | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Glue:: 毫升變換 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Grafana::Workspace | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::GreengrassV2::ComponentVersion | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::GroundStation::Config | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::GroundStation::DataflowEndpoint集團 | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::GroundStation::MissionProfile | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::GuardDuty::Detector | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::GuardDuty::Filter | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Guard責任:: 集 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::GuardDuty::ThreatIntel套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::IAM::Group | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::IAM::Policy | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::IAM::Role | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::IAM::User | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::IVS::Channel | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IVS::PlaybackKey一對 | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IVS::RecordingConfiguration | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::ImageBuilder::ContainerRecipe | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::ImageBuilder::DistributionConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ImageBuilder::ImagePipeline | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ImageBuilder::ImageRecipe | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ImageBuilder::InfrastructureConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::InspectorV2::Filter | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::IoT::AccountAudit配置 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::Authorizer | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT:: 緩存 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoT::CustomMetric | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::Dimension | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::FleetMetric | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::JobTemplate | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::MitigationAction | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::Policy | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::ProvisioningTemplate | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::RoleAlias | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoT::ScheduledAudit | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoT::SecurityProfile | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTAnalytics::Channel | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTAnalytics::Dataset | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTAnalytics::Datastore | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTAnalytics::Pipeline | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTEvents::AlarmModel | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTEvents::DetectorModel | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoTEvents::Input | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::IoTSiteWise::AssetModel | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTSiteWise::Dashboard | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTSiteWise::Gateway | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTSiteWise::Portal | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTSiteWise::Project | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTTwinMaker::ComponentType | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTTwinMaker::Entity | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoTTwinMaker::Scene | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTTwinMaker::SyncJob | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTTwinMaker::Workspace | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTWireless::FuotaTask | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTWireless::MulticastGroup | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::IoTWireless::ServiceProfile | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::KMS::Alias | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::KMS::Key | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::KafkaConnect::Connector | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Kendra::Index | 否 | 否 | 是 | 否 | 是 | 否 | 否 | 否 |
| AWS::Kinesis::Stream | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Kinesis::StreamConsumer | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::KinesisAnalyticsV2::Application | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::KinesisFirehose::DeliveryStream | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::KinesisVideo::SignalingChannel | 否 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::KinesisVideo::Stream | 否 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Lambda::CodeSigningConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Lambda::Function | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Lex::Bot | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Lex::BotAlias | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Lightsail::Bucket | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Lightsail::Certificate | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Lightsail::Disk | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Lightsail::StaticIp | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Logs::Destination | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::LookoutMetrics::Alert | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::LookoutVision::Project | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::M2::Environment | 否 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::MSK::BatchScram秘密 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MSK::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MSK::ClusterPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MSK::Configuration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::MSK::VpcConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MediaConnect::FlowEntitlement | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::MediaConnect::FlowSource | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::MediaConnect::FlowVpc介面 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::MediaPackage::PackagingConfiguration | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::MediaPackage::PackagingGroup | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::MediaTailor::PlaybackConfiguration | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::MemoryDB::SubnetGroup | 是 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::NetworkFirewall::Firewall | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::NetworkFirewall::FirewallPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::NetworkFirewall::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Network防火牆:: TLSInspectionConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::OpenSearch::Domain | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Panorama::Package | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::Personalize::Dataset | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::Personalize::DatasetGroup | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Personalize::Schema | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::Personalize::Solution | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::Pinpoint::App | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Pinpoint::ApplicationSettings | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Pinpoint::Campaign | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Pinpoint::EmailChannel | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Pinpoint::EmailTemplate | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Pinpoint::EventStream | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Pinpoint::InApp。模板 | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Pinpoint::Segment | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::QLDB::Ledger | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::QuickSight::DataSource | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::QuickSight::Template | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::QuickSight::Theme | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::RDS::DBCluster | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 |
| AWS:: RDS:: 資料庫 ClusterSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::RDS::DBInstance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SecurityGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::DBSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SubnetGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::GlobalCluster | 否 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::RDS::OptionGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RUM::AppMonitor | 是 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Redshift::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterParameter集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSecurity集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSubnet集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::EndpointAccess | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Redshift::EndpointAuthorization | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::Redshift::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲(愛爾蘭) | 歐洲(法蘭克福) | 歐洲(倫敦) | 歐洲(巴黎) | 歐洲(斯德哥爾摩) | 歐洲(米蘭) | 歐洲(西班牙) | 歐洲(蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Redshift::ScheduledAction | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ResilienceHub::App | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ResilienceHub::ResiliencyPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ResourceExplorer2::Index | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::RoboMaker::RobotApplication | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::RoboMaker::RobotApplication版本 | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::RoboMaker::SimulationApplication | 否 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| AWS::Route53Resolver::FirewallDomain列表 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Route53Resolver::FirewallRule集團 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::ResolverEndpoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig協會 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::ResolverRule | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Route53Resolver::ResolverRule協會 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::S3::AccessPoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::S3::AccountPublicAccessBlock | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::S3::Bucket | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::S3::StorageLens | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::SES::ConfigurationSet | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SES::ContactList | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SES::ReceiptFilter | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::SES::ReceiptRule套裝 | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::SES::Template | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::SNS::Topic | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SQS::Queue | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SSM::AssociationCompliance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SSM::Document | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SSM::FileData | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SSM::ManagedInstance庫存 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SSM::PatchCompliance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SageMaker::AppImageConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::CodeRepository | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SageMaker::Domain | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SageMaker::EndpointConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SageMaker::FeatureGroup | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SageMaker::Image | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SageMaker::Model | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SageMaker::NotebookInstance | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::Workteam | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::SecretsManager::Secret | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceCatalog::CloudFormation产品 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceCatalog::Portfolio | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceDiscovery::HttpNamespace | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ServiceDiscovery::Instance | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ServiceDiscovery::PublicDns名稱區 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::ServiceDiscovery::Service | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::ShieldRegional::Protection | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Signer::SigningProfile | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::StepFunctions::Activity | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::StepFunctions::StateMachine | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Transfer::Agreement | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Transfer::Certificate | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::Transfer::Connector | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::Transfer::Profile | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Transfer::Workflow | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| AWS::WAFRegional::RateBased規則 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::Rule | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::WebACL | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::IPSet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::ManagedRule套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 歐洲 (愛爾蘭) | 歐洲 (法蘭克福) | 歐洲 (倫敦) | 歐洲 (巴黎) | 歐洲 (斯德哥爾摩) | 歐洲 (米蘭) | 歐洲 (西班牙) | 歐洲 (蘇黎世) |
|---|---|---|---|---|---|---|---|---|
| AWS::WAFv2::RegexPattern套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::WebACL | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WorkSpaces::ConnectionAlias | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::WorkSpaces::Workspace | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| AWS::XRay::EncryptionConfig | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

# 亞太區域

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ACM::Certificate | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ACMPCA::CertificateAuthority | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ACMPCA::CertificateAuthority激活 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::APS::RuleGroups名稱區 | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::AccessAnalyzer::Analyzer | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AmazonMQ::Broker | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Amplify::App | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Amplify::Branch | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ApiGateway::RestApi | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ApiGateway::Stage | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ApiGatewayV2::Api | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ApiGatewayV2::Stage | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AppConfig::Application | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AppConfig::ConfigurationProfile | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AppConfig::DeploymentStrategy | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::AppConfig::Environment | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AppConfig::ExtensionAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AppConfig::HostedConfiguration版本 | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AppFlow::Flow | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::AppIntegrations::EventIntegration | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::AppMesh::GatewayRoute | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::AppMesh::Mesh | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::AppMesh::Route | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::AppMesh::VirtualGateway | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::AppMesh::VirtualNode | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::AppMesh::VirtualRouter | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::AppMesh::VirtualService | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::AppRunner::Service | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::AppRunner::VpcConnector | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 否 |
| AWS::AppStream::Application | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::AppStream::DirectoryConfig | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::AppStream::Fleet | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::AppStream::Stack | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::AppSync::GraphQLapi | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Athena::DataCatalog | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Athena::PreparedStatement | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Athena::WorkGroup | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::AuditManager::Assessment | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::AutoScaling::AutoScaling集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::AutoScaling::LaunchConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::ScalingPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::ScheduledAction | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Auto Scaling::WarmPool | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Back up::BackupPlan | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Back up::BackupSelection | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Back up::BackupVault | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Back up::RecoveryPoint | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Backup::ReportPlan | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Batch::ComputeEnvironment | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Batch::JobQueue | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Batch::SchedulingPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Cassandra::Keyspace | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Cloud9::EnvironmentEC2 | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::CloudFormation::Stack | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::CloudTrail::Trail | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::CloudWatch::Alarm | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::CloudWatch::MetricStream | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::CodeArtifact::Repository | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::CodeBuild::Project | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::CodeBuild::ReportGroup | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::CodeDeploy::Application | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::CodeDeploy::DeploymentConfig | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::CodeDeploy::DeploymentGroup | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::CodeGuruProfiler::ProfilingGroup | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::CodeGuruReviewer::RepositoryAssociation | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::CodePipeline::Pipeline | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Cognito::UserPool | 是 | 否 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Cognito::UserPool客戶 | 是 | 否 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Cognito::UserPool集團 | 是 | 否 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Config::ConfigurationRecorder | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Config::ConformancePack合規 | 是 | 否 | 是 | 否 | 是 | 否 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Config::ResourceCompliance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Connect::Instance | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Connect::PhoneNumber | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Connect::QuickConnect | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::CustomerProfiles::Domain | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::CustomerProfiles::ObjectType | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::DMS::Certificate | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DMS::Endpoint | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::DMS::EventSubscription | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DMS::ReplicationInstance | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DMS::ReplicationSubnet集團 | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DMS::ReplicationTask | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DataSync::LocationEFS | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DataSync::LocationF SxLustre | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DataSync::LocationF SxWindows | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DataSync::LocationHDFS | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::DataSync::LocationNFS | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::DataSync::LocationObject儲存 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DataSync::LocationS3 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DataSync::Location中小企 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::DataSync::Task | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Detective::Graph | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::DynamoDB::Table | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Capacity Reservation | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::CarrierGateway | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 否 | 是 |
| AWS::EC2::ClientVpn端點 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::CustomerGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::DHCPOptions | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::EC2::EC2Fleet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::EIP | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::EgressOnlyInternetGateway | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::EC2::FlowLog | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::Host | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::IPAM | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::IPAMPool | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::IPAMScope | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Instance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::InternetGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::LaunchTemplate | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::EC2::NatGateway | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::NetworkAcl | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::NetworkInsightsAccessScope | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::NetworkInsightsAccessScope分析 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::NetworkInsights分析 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::NetworkInsights路徑 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::NetworkInterface | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::PrefixList | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Registered哈實例 | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::RouteTable | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SecurityGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SpotFleet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Subnet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::SubnetRouteTableAssociation | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::TrafficMirror過濾器 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::TrafficMirror階段 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::TrafficMirror目標 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::TransitGateway | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EC2::TransitGateway附件 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::EC2::TransitGatewayConnect | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::EC2::TransitGatewayMulticastDomain | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::TransitGatewayRouteTable | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::EC2::VPC | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPCEndpoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: EC2:: VPC EndpointService | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS:: EC2:: VPC PeeringConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPNConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::VPNGateway | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EC2::Volume | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECR::PullThroughCacheRule | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECR::RegistryPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECR::Repository | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::CapacityProvider | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ECS::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::Service | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::TaskDefinition | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ECS::TaskSet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EFS::AccessPoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EFS::FileSystem | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EKS::Addon | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EKS::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EKS::FargateProfile | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EKS::IdentityProviderConfig | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EMR::SecurityConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ElasticBeanstalk::Application | 是 | 是 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ElasticBeanstalk::ApplicationVersion | 是 | 是 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ElasticBeanstalk::Environment | 是 | 是 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ElasticLoadBalancing::LoadBalancer | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ElasticLoadBalancingV2::Listener | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ElasticLoadBalancingV2::LoadBalancer | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Elasticsearch::Domain | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::EventSchemas::Discoverer | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EventSchemas::Registry | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EventSchemas::RegistryPolicy | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::EventSchemas::Schema | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Events::ApiDestination | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Events::Archive | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Events::Connection | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Events::Endpoint | 是 | 否 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Events::EventBus | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Events::Rule | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Evidently::Launch | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::Evidently::Project | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::Evidently::Segment | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::FIS::ExperimentTemplate | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Forecast::Dataset | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Forecast::DatasetGroup | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::FraudDetector::EntityType | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::FraudDetector::Label | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::FraudDetector::Outcome | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::FraudDetector::Variable | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::Glue::Classifier | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Glue::Job | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Glue:: 毫升變換 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Grafana::Workspace | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::GreengrassV2::ComponentVersion | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::GroundStation::Config | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 是 | 是 |
| AWS::GroundStation::DataflowEndpoint集團 | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 是 | 是 |
| AWS::GroundStation::MissionProfile | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 是 | 是 |
| AWS::GuardDuty::Detector | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::GuardDuty::Filter | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Guard責任:: 集 | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::GuardDuty::ThreatIntel套裝 | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Health湖:: F | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 |
| AWS::IAM::Group | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::IAM::Policy | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::IAM::Role | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::IAM::User | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::IVS::Channel | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 否 | 否 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IVS::PlaybackKey一對 | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 否 | 否 |
| AWS::IVS::RecordingConfiguration | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 否 | 否 |
| AWS::ImageBuilder::ContainerRecipe | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ImageBuilder::DistributionConfiguration | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::ImageBuilder::ImagePipeline | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ImageBuilder::ImageRecipe | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::ImageBuilder::InfrastructureConfiguration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::InspectorV2::Filter | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoT::AccountAudit配置 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::Authorizer | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT:: 緩存 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::CustomMetric | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::Dimension | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::FleetMetric | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::JobTemplate | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::MitigationAction | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoT::Policy | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::ProvisioningTemplate | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::RoleAlias | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::ScheduledAudit | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoT::SecurityProfile | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTAnalytics::Channel | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 是 |
| AWS::IoTAnalytics::Dataset | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 是 |
| AWS::IoTAnalytics::Datastore | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoTAnalytics::Pipeline | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 是 |
| AWS::IoTEvents::AlarmModel | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTEvents::DetectorModel | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTEvents::Input | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTSiteWise::AssetModel | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTSiteWise::Dashboard | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTSiteWise::Gateway | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTSiteWise::Portal | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoTSiteWise::Project | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::IoTTwinMaker::ComponentType | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::IoTTwinMaker::Entity | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::IoTTwinMaker::Scene | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::IoTTwinMaker::SyncJob | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::IoTTwinMaker::Workspace | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::IoTWireless::FuotaTask | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 是 |
| AWS::IoTWireless::MulticastGroup | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoTWireless::ServiceProfile | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 是 |
| AWS::KMS::Alias | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::KMS::Key | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::KafkaConnect::Connector | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Kendra::Index | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::Kinesis::Stream | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Kinesis::StreamConsumer | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::KinesisAnalyticsV2::Application | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::KinesisFirehose::DeliveryStream | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::KinesisVideo::SignalingChannel | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::KinesisVideo::Stream | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Lambda::CodeSigningConfig | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Lambda::Function | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Lex::Bot | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Lex::BotAlias | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Lightsail::Bucket | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Lightsail::Certificate | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Lightsail::Disk | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Lightsail::StaticIp | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Logs::Destination | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::LookoutMetrics::Alert | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::LookoutVision::Project | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 否 | 否 |
| AWS::M2::Environment | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::MSK::BatchScram秘密 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::MSK::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MSK::ClusterPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MSK::Configuration | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MSK::VpcConnection | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::MediaConnect::FlowEntitlement | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::MediaConnect::FlowSource | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::MediaConnect::FlowVpc介面 | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::MediaPackage::PackagingConfiguration | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::MediaPackage::PackagingGroup | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::MediaTailor::PlaybackConfiguration | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::MemoryDB::SubnetGroup | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::NetworkFirewall::Firewall | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::NetworkFirewall::FirewallPolicy | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::NetworkFirewall::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Network防火牆:: TLS InspectionConfiguration | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::OpenSearch::Domain | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Panorama::Package | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| AWS::Personalize::Dataset | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Personalize::DatasetGroup | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Personalize::Schema | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Personalize::Solution | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Pinpoint::App | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Pinpoint::ApplicationSettings | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Pinpoint::Campaign | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Pinpoint::EmailChannel | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Pinpoint::EmailTemplate | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Pinpoint::EventStream | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Pinpoint::InApp。模板 | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Pinpoint::Segment | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::QLDB::Ledger | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::QuickSight::DataSource | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::QuickSight::Template | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::QuickSight::Theme | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::RDS::DBCluster | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 ClusterSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::DBInstance | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SecurityGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::DBSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SubnetGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RDS::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::RDS::GlobalCluster | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::RDS::OptionGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::RUM::AppMonitor | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 是 |
| AWS::Redshift::Cluster | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterParameter集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSecurity集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSnapshot | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSubnet集團 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Redshift::EndpointAccess | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Redshift::EndpointAuthorization | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::Redshift::EventSubscription | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ScheduledAction | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ResilienceHub::App | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ResilienceHub::ResiliencyPolicy | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ResourceExplorer2::Index | 是 | 否 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::RoboMaker::RobotApplication | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 否 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::RoboMaker::RobotApplication版本 | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✓ 是 | ✓ 是 | ✗ 否 |
| AWS::RoboMaker::SimulationApplication | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✗ 否 | ✓ 是 | ✓ 是 | ✗ 否 |
| AWS::Route53Resolver::FirewallDomain列表 | ✓ 是 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✓ 是 |
| AWS::Route53Resolver::FirewallRule集團 | ✓ 是 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✓ 是 |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | ✓ 是 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✓ 是 |
| AWS::Route53Resolver::ResolverEndpoint | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✓ 是 | ✓ 是 | ✓ 是 | ✓ 是 | ✓ 是 | ✓ 是 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | ✓ 是 | ✗ 否 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✓ 是 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig協會 | ✓ 是 | ✗ 否 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✗ 否 | ✓ 是 | ✓ 是 | ✓ 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Route53Resolver::ResolverRule | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Route53Resolver::ResolverRule協會 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::S3::AccessPoint | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::S3::AccountPublicAccessBlock | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::S3::Bucket | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::S3::StorageLens | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::SES::ConfigurationSet | 是 | 是 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SES::ContactList | 是 | 是 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::SES::Template | 是 | 是 | 否 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SNS::Topic | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SQS::Queue | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SSM::AssociationCompliance | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 |
| AWS::SSM::Document | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SSM::FileData | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 |
| AWS::SSM::ManagedInstance庫存 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::SSM::PatchCompliance | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::AppImageConfig | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::CodeRepository | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::Domain | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::EndpointConfig | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::FeatureGroup | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::Image | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::Model | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::NotebookInstance | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::NotebookInstanceLifecycleConfig | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::SageMaker::Workteam | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::SecretsManager::Secret | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceCatalog::CloudFormation产品 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceCatalog::Portfolio | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::ServiceDiscovery::HttpNamespace | 是 | 否 | 是 | 否 | 是 | 否 | 是 | 是 | 是 | 是 |
| AWS::ServiceDiscovery::Instance | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ServiceDiscovery::PublicDns命名空 | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ServiceDiscovery::Service | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::ShieldRegional::Protection | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Signer::SigningProfile | 是 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::StepFunctions::Activity | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::StepFunctions::StateMachine | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Transfer::Agreement | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Transfer::Certificate | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Transfer::Connector | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::Transfer::Profile | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::Transfer::Workflow | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 是 |
| AWS::WAFRegional::RateBased規則 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::Rule | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::WebACL | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::IPSet | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 亞太區域(新加坡) | 亞太區域(東京) | 亞太區域(雪梨) | 亞太區域(首爾) | 亞太區域(孟買) | 亞太區域(大阪) | 亞太區域(香港) | 亞太區域(雅加達) | 亞太區域(海德拉巴) | 亞太區域(墨爾本) |
|---|---|---|---|---|---|---|---|---|---|---|
| AWS::WAFv2::ManagedRule套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::RegexPattern套裝 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::RuleGroup | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::WebACL | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| AWS::WorkSpaces::ConnectionAlias | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::WorkSpaces::Workspace | 是 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 是 | 是 |
| AWS::XRay::EncryptionConfig | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

# 中國區域

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::ACM::Certificate | 是 | 是 |
| AWS::AmazonMQ::Broker | 是 | 是 |
| AWS::ApiGateway::RestApi | 是 | 是 |
| AWS::ApiGateway::Stage | 是 | 是 |
| AWS::ApiGatewayV2::Api | 是 | 是 |
| AWS::ApiGatewayV2::Stage | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::AppConfig::Application | 是 | 是 |
| AWS::AppConfig::ConfigurationProfile | 是 | 是 |
| AWS::AppConfig::DeploymentStrategy | 是 | 是 |
| AWS::AppConfig::Environment | 是 | 是 |
| AWS::AppConfig::ExtensionAssociation | 是 | 是 |
| AWS::AppConfig::HostedConfiguration版本 | 是 | 是 |
| AWS::AppSync::GraphQLapi | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::Athena::DataCatalog | 是 | 是 |
| AWS::Athena::PreparedStatement | 是 | 是 |
| AWS::Athena::WorkGroup | 是 | 是 |
| AWS::AutoScaling::AutoScaling集團 | 是 | 是 |
| AWS::AutoScaling::LaunchConfiguration | 是 | 是 |
| AWS::AutoScaling::ScalingPolicy | 是 | 是 |
| AWS::AutoScaling::ScheduledAction | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::AutoScaling::WarmPool | 是 | 是 |
| AWS::Backup::BackupPlan | 是 | 是 |
| AWS::Backup::BackupSelection | 是 | 是 |
| AWS::Backup::BackupVault | 是 | 是 |
| AWS::Backup::RecoveryPoint | 是 | 是 |
| AWS::Batch::ComputeEnvironment | 是 | 是 |
| AWS::Batch::JobQueue | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::Batch::SchedulingPolicy | 是 | 是 |
| AWS::Cassandra::Keyspace | 是 | 是 |
| AWS::CloudFormation::Stack | 是 | 是 |
| AWS::CloudTrail::Trail | 是 | 是 |
| AWS::CloudWatch::Alarm | 是 | 是 |
| AWS::CloudWatch::MetricStream | 是 | 是 |
| AWS::CodeBuild::Project | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::CodeBuild::ReportGroup | 是 | 是 |
| AWS::Config::ConfigurationRecorder | 是 | 是 |
| AWS::Config::ResourceCompliance | 是 | 是 |
| AWS::DMS::Certificate | 是 | 是 |
| AWS::DMS::Endpoint | 是 | 是 |
| AWS::DMS::EventSubscription | 是 | 是 |
| AWS::DMS::ReplicationInstance | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::DMS::ReplicationSubnet集團 | 是 | 是 |
| AWS::DMS::ReplicationTask | 是 | 是 |
| AWS::DataSync::LocationEFS | 是 | 是 |
| AWS::DataSync::LocationHDFS | 是 | 是 |
| AWS::DataSync::LocationNFS | 是 | 是 |
| AWS::DataSync::LocationObject儲存 | 是 | 是 |
| AWS::DataSync::LocationS3 | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::DataSync::Location中小企 | 是 | 是 |
| AWS::DataSync::Task | 是 | 是 |
| AWS::DynamoDB::Table | 是 | 是 |
| AWS::EC2::CapacityReservation | 是 | 是 |
| AWS::EC2::DHCPOptions | 是 | 是 |
| AWS::EC2::EC2Fleet | 是 | 是 |
| AWS::EC2::EIP | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::EC2::FlowLog | 是 | 是 |
| AWS::EC2::Host | 是 | 是 |
| AWS::EC2::Instance | 是 | 是 |
| AWS::EC2::InternetGateway | 是 | 是 |
| AWS::EC2::LaunchTemplate | 是 | 是 |
| AWS::EC2::NatGateway | 是 | 是 |
| AWS::EC2::NetworkAcl | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::EC2::NetworkInterface | 是 | 是 |
| AWS::EC2::PrefixList | 是 | 是 |
| AWS::EC2::RouteTable | 是 | 是 |
| AWS::EC2::SecurityGroup | 是 | 是 |
| AWS::EC2::SpotFleet | 是 | 是 |
| AWS::EC2::Subnet | 是 | 是 |
| AWS::EC2::SubnetRouteTableAssociation | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::EC2::TrafficMirror過濾器 | 是 | 是 |
| AWS::EC2::TrafficMirror階段 | 是 | 是 |
| AWS::EC2::TrafficMirror目標 | 是 | 是 |
| AWS::EC2::TransitGateway | 是 | 是 |
| AWS::EC2::TransitGateway附件 | 是 | 是 |
| AWS::EC2::TransitGatewayConnect | 是 | 是 |
| AWS::EC2::TransitGatewayMulticastDomain | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::EC2::TransitGatewayRouteTable | 是 | 是 |
| AWS::EC2::VPC | 是 | 是 |
| AWS::EC2::VPCEndpoint | 是 | 是 |
| AWS:: EC2:: VPC EndpointService | 是 | 是 |
| AWS:: EC2:: VPC PeeringConnection | 是 | 是 |
| AWS::EC2::VPNGateway | 是 | 否 |
| AWS::EC2::Volume | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::ECR::Repository | 是 | 是 |
| AWS::ECS::CapacityProvider | 是 | 是 |
| AWS::ECS::Cluster | 是 | 是 |
| AWS::ECS::Service | 是 | 是 |
| AWS::ECS::TaskDefinition | 是 | 是 |
| AWS::ECS::TaskSet | 是 | 是 |
| AWS::EFS::AccessPoint | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::EFS::FileSystem | 是 | 是 |
| AWS::EKS::Addon | 是 | 是 |
| AWS::EKS::Cluster | 是 | 是 |
| AWS::EKS::FargateProfile | 是 | 是 |
| AWS::EKS::IdentityProviderConfig | 是 | 是 |
| AWS::EMR::SecurityConfiguration | 是 | 是 |
| AWS::ElasticBeanstalk::Application | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::ElasticBeanstalk::ApplicationVersion | 是 | 是 |
| AWS::ElasticBeanstalk::Environment | 是 | 是 |
| AWS::ElasticLoadBalancing::LoadBalancer | 是 | 是 |
| AWS::ElasticLoadBalancingV2::Listener | 是 | 是 |
| AWS::ElasticLoadBalancingV2::LoadBalancer | 是 | 是 |
| AWS::Elasticsearch::Domain | 是 | 是 |
| AWS::Events::Archive | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::Events::EventBus | 是 | 是 |
| AWS::Events::Rule | 是 | 是 |
| AWS::Glue::Classifier | 是 | 是 |
| AWS::Glue::Job | 是 | 是 |
| AWS::Glue:: 毫升變換 | 是 | 否 |
| AWS::GreengrassV2::ComponentVersion | 是 | 否 |
| AWS::GuardDuty::Filter | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::GuardDuty::ThreatIntel套裝 | 是 | 是 |
| AWS::IAM::Group | 是 | 是 |
| AWS::IAM::InstanceProfile | 是 | 否 |
| AWS::IAM::OIDCProvider | 是 | 否 |
| AWS::IAM::Policy | 是 | 是 |
| AWS::IAM::Role | 是 | 是 |
| AWS::IAM::SAMLProvider | 是 | 否 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::IAM::ServerCertificate | 是 | 否 |
| AWS::IAM::User | 是 | 是 |
| AWS::ImageBuilder::ContainerRecipe | 是 | 是 |
| AWS::ImageBuilder::DistributionConfiguration | 是 | 是 |
| AWS::ImageBuilder::ImagePipeline | 是 | 是 |
| AWS::ImageBuilder::ImageRecipe | 是 | 是 |
| AWS::ImageBuilder::InfrastructureConfiguration | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::IoT::AccountAudit配置 | 是 | 是 |
| AWS::IoT::Authorizer | 是 | 是 |
| AWS::IoT:: 緩存 | 是 | 是 |
| AWS::IoT::CustomMetric | 是 | 是 |
| AWS::IoT::Dimension | 是 | 是 |
| AWS::IoT::FleetMetric | 是 | 是 |
| AWS::IoT::JobTemplate | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::IoT::MitigationAction | 是 | 是 |
| AWS::IoT::Policy | 是 | 是 |
| AWS::IoT::ProvisioningTemplate | 是 | 是 |
| AWS::IoT::RoleAlias | 是 | 是 |
| AWS::IoT::ScheduledAudit | 是 | 是 |
| AWS::IoT::SecurityProfile | 是 | 是 |
| AWS::IoTAnalytics::Channel | 是 | 否 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::IoTAnalytics::Dataset | 是 | 否 |
| AWS::IoTAnalytics::Datastore | 是 | 否 |
| AWS::IoTAnalytics::Pipeline | 是 | 否 |
| AWS::IoTEvents::AlarmModel | 是 | 否 |
| AWS::IoTEvents::DetectorModel | 是 | 否 |
| AWS::IoTEvents::Input | 是 | 否 |
| AWS::IoTSiteWise::AssetModel | 是 | 否 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::IoTSiteWise::Dashboard | 是 | 否 |
| AWS::IoTSiteWise::Gateway | 是 | 否 |
| AWS::IoTSiteWise::Portal | 是 | 否 |
| AWS::IoTSiteWise::Project | 是 | 否 |
| AWS::KMS::Alias | 是 | 是 |
| AWS::KMS::Key | 是 | 是 |
| AWS::Kinesis::Stream | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::Kinesis::StreamConsumer | 是 | 是 |
| AWS::KinesisAnalyticsV2::Application | 是 | 是 |
| AWS::KinesisFirehose::DeliveryStream | 是 | 是 |
| AWS::Lambda::Function | 是 | 否 |
| AWS::Logs::Destination | 是 | 是 |
| AWS::MSK::BatchScram秘密 | 是 | 是 |
| AWS::MSK::Cluster | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::MSK::ClusterPolicy | 是 | 是 |
| AWS::MSK::Configuration | 是 | 是 |
| AWS::MSK::VpcConnection | 是 | 是 |
| AWS::NetworkFirewall::Firewall | 是 | 是 |
| AWS::NetworkFirewall::FirewallPolicy | 是 | 是 |
| AWS::NetworkFirewall::RuleGroup | 是 | 是 |
| AWS::Network防火牆:: TLS InspectionConfiguration | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::OpenSearch::Domain | 是 | 是 |
| AWS::Personalize::Dataset | 是 | 否 |
| AWS::Personalize::DatasetGroup | 是 | 否 |
| AWS::Personalize::Schema | 是 | 否 |
| AWS::Personalize::Solution | 是 | 否 |
| AWS::RDS::DBCluster | 否 | 是 |
| AWS:: RDS:: 資料庫 ClusterSnapshot | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::RDS::DBInstance | 是 | 是 |
| AWS:: RDS:: 資料庫 SecurityGroup | 是 | 是 |
| AWS::RDS::DBSnapshot | 是 | 是 |
| AWS:: RDS:: 資料庫 SubnetGroup | 是 | 是 |
| AWS::RDS::EventSubscription | 是 | 是 |
| AWS::RDS::OptionGroup | 是 | 是 |
| AWS::Redshift::Cluster | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::Redshift::ClusterParameter集團 | 是 | 是 |
| AWS::Redshift::ClusterSecurity集團 | 是 | 是 |
| AWS::Redshift::ClusterSnapshot | 是 | 是 |
| AWS::Redshift::ClusterSubnet集團 | 是 | 是 |
| AWS::Redshift::EventSubscription | 是 | 是 |
| AWS::Route53Resolver::FirewallDomain列表 | 是 | 是 |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::Route53Resolver::ResolverEndpoint | 是 | 是 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | 是 | 是 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig協會 | 是 | 是 |
| AWS::Route53Resolver::ResolverRule | 是 | 是 |
| AWS::Route53Resolver::ResolverRule協會 | 是 | 是 |
| AWS::S3::AccessPoint | 是 | 是 |
| AWS::S3::AccountPublicAccessBlock | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::S3::Bucket | 是 | 是 |
| AWS::SES::ConfigurationSet | 否 | 是 |
| AWS::SES::ContactList | 否 | 是 |
| AWS::SES::Template | 否 | 是 |
| AWS::SNS::Topic | 是 | 是 |
| AWS::SQS::Queue | 是 | 是 |
| AWS::SSM::AssociationCompliance | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::SSM::Document | 是 | 是 |
| AWS::SSM::FileData | 是 | 是 |
| AWS::SSM::ManagedInstance庫存 | 是 | 是 |
| AWS::SSM::PatchCompliance | 是 | 是 |
| AWS::SageMaker::AppImageConfig | 是 | 是 |
| AWS::SageMaker::CodeRepository | 是 | 是 |
| AWS::SageMaker::Domain | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::SageMaker::EndpointConfig | 是 | 是 |
| AWS::SageMaker::FeatureGroup | 是 | 是 |
| AWS::SageMaker::Image | 是 | 是 |
| AWS::SageMaker::Model | 是 | 是 |
| AWS::SageMaker::NotebookInstance | 是 | 是 |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | 是 | 是 |
| AWS::SecretsManager::Secret | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::ServiceCatalog::CloudFormation产品 | 是 | 是 |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | 是 | 是 |
| AWS::ServiceCatalog::Portfolio | 是 | 是 |
| AWS::ServiceDiscovery::HttpNamespace | 是 | 是 |
| AWS::ServiceDiscovery::Instance | 是 | 是 |
| AWS::ServiceDiscovery::PublicDns命名空 | 是 | 是 |
| AWS::ServiceDiscovery::Service | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::StepFunctions::Activity | 是 | 否 |
| AWS::StepFunctions::StateMachine | 是 | 是 |
| AWS::Transfer::Agreement | 是 | 是 |
| AWS::Transfer::Certificate | 是 | 是 |
| AWS::Transfer::Connector | 是 | 是 |
| AWS::Transfer::Profile | 是 | 是 |
| AWS::Transfer::Workflow | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::WAFRegional::RateBased規則 | 是 | 是 |
| AWS::WAFRegional::Rule | 是 | 是 |
| AWS::WAFRegional::RuleGroup | 是 | 是 |
| AWS::WAFRegional::WebACL | 是 | 是 |
| AWS::WAFv2::IPSet | 是 | 是 |
| AWS::WAFv2::ManagedRule套裝 | 是 | 是 |
| AWS::WAFv2::RegexPattern套裝 | 是 | 是 |

| Resource Type (資源類型) | 中國 (北京) | 中國 (寧夏) |
| --- | --- | --- |
| AWS::WAFv2::RuleGroup | 是 | 是 |
| AWS::WAFv2::WebACL | 是 | 是 |
| AWS::WorkSpaces::Workspace | 否 | 是 |

## 非洲和中東區域

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
| --- | --- | --- | --- | --- |
| AWS::ACM::Certificate | 是 | 是 | 是 | 是 |
| AWS::ACMPCA::CertificateAuthority | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ACMPCA::CertificateAuthority激活 | 是 | 是 | 是 | 否 |
| AWS::AccessAnalyzer::Analyzer | 是 | 是 | 是 | 否 |
| AWS::AmazonMQ::Broker | 是 | 是 | 是 | 否 |
| AWS::Amplify::App | 是 | 否 | 否 | 否 |
| AWS::Amplify::Branch | 是 | 否 | 否 | 否 |
| AWS::ApiGateway::RestApi | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ApiGateway::Stage | 是 | 是 | 是 | 是 |
| AWS::ApiGatewayV2::Api | 是 | 是 | 是 | 是 |
| AWS::ApiGatewayV2::Stage | 是 | 是 | 是 | 是 |
| AWS::AppConfig::Application | 是 | 是 | 否 | 是 |
| AWS::AppConfig::ConfigurationProfile | 是 | 是 | 否 | 是 |
| AWS::AppConfig::DeploymentStrategy | 是 | 是 | 否 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::AppConfig::Environment | 是 | 是 | 否 | 是 |
| AWS::AppConfig::ExtensionAssociation | 是 | 是 | 是 | 是 |
| AWS::AppConfig::HostedConfiguration版本 | 是 | 是 | 否 | 是 |
| AWS::AppIntegrations::EventIntegration | 否 | 是 | 否 | 否 |
| AWS::AppMesh::GatewayRoute | 是 | 是 | 否 | 否 |
| AWS::AppMesh::Mesh | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::AppMesh::Route | 是 | 是 | 否 | 否 |
| AWS::AppMesh::VirtualGateway | 是 | 是 | 否 | 否 |
| AWS::AppMesh::VirtualNode | 是 | 是 | 否 | 否 |
| AWS::AppMesh::VirtualRouter | 是 | 是 | 否 | 否 |
| AWS::AppMesh::VirtualService | 是 | 是 | 否 | 否 |
| AWS::AppSync::GraphQLapi | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Athena::DataCatalog | 是 | 是 | 是 | 否 |
| AWS::Athena::PreparedStatement | 是 | 是 | 否 | 否 |
| AWS::Athena::WorkGroup | 是 | 是 | 是 | 否 |
| AWS::AutoScaling::AutoScaling集團 | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::LaunchConfiguration | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::ScalingPolicy | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::AutoScaling::ScheduledAction | 是 | 是 | 是 | 是 |
| AWS::AutoScaling::WarmPool | 是 | 是 | 否 | 否 |
| AWS::Backup::BackupPlan | 是 | 是 | 否 | 否 |
| AWS::Backup::BackupSelection | 是 | 是 | 是 | 否 |
| AWS::Backup::BackupVault | 是 | 是 | 是 | 否 |
| AWS::Backup::RecoveryPoint | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Backup::ReportPlan | 是 | 是 | 否 | 否 |
| AWS::Batch::ComputeEnvironment | 是 | 是 | 是 | 否 |
| AWS::Batch::JobQueue | 是 | 是 | 是 | 否 |
| AWS::Batch::SchedulingPolicy | 是 | 是 | 是 | 否 |
| AWS::Cassandra::Keyspace | 是 | 否 | 否 | 否 |
| AWS::Cloud9::EnvironmentEC2 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::CloudFormation::Stack | 是 | 是 | 否 | 否 |
| AWS::CloudTrail::Trail | 是 | 是 | 是 | 是 |
| AWS::CloudWatch::Alarm | 是 | 是 | 是 | 是 |
| AWS::CloudWatch::MetricStream | 是 | 是 | 是 | 是 |
| AWS::CodeBuild::Project | 是 | 是 | 是 | 是 |
| AWS::CodeBuild::ReportGroup | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::CodeDeploy::Application | 是 | 是 | 否 | 否 |
| AWS::CodeDeploy::DeploymentConfig | 是 | 是 | 否 | 否 |
| AWS::CodeDeploy::DeploymentGroup | 是 | 是 | 否 | 否 |
| AWS::Cognito::UserPool | 是 | 否 | 否 | 是 |
| AWS::Cognito::UserPool客戶 | 是 | 否 | 否 | 是 |
| AWS::Cognito::UserPool集團 | 是 | 否 | 否 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Config::ConfigurationRecorder | 是 | 是 | 是 | 是 |
| AWS::Config::ConformancePack合規 | 是 | 否 | 否 | 否 |
| AWS::Config::ResourceCompliance | 是 | 是 | 是 | 是 |
| AWS::Connect::Instance | 否 | 是 | 否 | 否 |
| AWS::CustomerProfiles::Domain | 否 | 是 | 否 | 否 |
| AWS::CustomerProfiles::ObjectType | 否 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::DMS::Certificate | 是 | 是 | 否 | 否 |
| AWS::DMS::Endpoint | 是 | 是 | 否 | 否 |
| AWS::DMS::EventSubscription | 是 | 是 | 否 | 否 |
| AWS::DMS::ReplicationInstance | 是 | 是 | 否 | 否 |
| AWS::DMS::ReplicationSubnet集團 | 是 | 是 | 否 | 否 |
| AWS::DMS::ReplicationTask | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::DataSync::LocationEFS | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationF SxLustre | 是 | 是 | 否 | 否 |
| AWS::DataSync::LocationF SxWindows | 是 | 是 | 否 | 否 |
| AWS::DataSync::LocationHDFS | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationNFS | 是 | 是 | 是 | 否 |
| AWS::DataSync::LocationObject儲存 | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::DataSync::LocationS3 | 是 | 是 | 是 | 否 |
| AWS::DataSync::Location中小企 | 是 | 是 | 是 | 否 |
| AWS::DataSync::Task | 是 | 是 | 是 | 否 |
| AWS::Detective::Graph | 是 | 是 | 否 | 否 |
| AWS::DynamoDB::Table | 是 | 是 | 是 | 是 |
| AWS::EC2::CapacityReservation | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EC2::ClientVpn端點 | 是 | 是 | 否 | 否 |
| AWS::EC2::CustomerGateway | 是 | 是 | 是 | 是 |
| AWS::EC2::DHCPOptions | 是 | 是 | 是 | 是 |
| AWS::EC2::EC2Fleet | 是 | 是 | 是 | 否 |
| AWS::EC2::EIP | 是 | 是 | 是 | 是 |
| AWS::EC2::EgressOnlyInternetGateway | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EC2::FlowLog | 是 | 是 | 是 | 否 |
| AWS::EC2::Host | 是 | 是 | 是 | 是 |
| AWS::EC2::IPAM | 是 | 是 | 是 | 否 |
| AWS::EC2::IPAMPool | 是 | 是 | 是 | 否 |
| AWS::EC2::IPAMScope | 是 | 是 | 是 | 否 |
| AWS::EC2::Instance | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EC2::InternetGateway | 是 | 是 | 是 | 是 |
| AWS::EC2::LaunchTemplate | 是 | 是 | 否 | 否 |
| AWS::EC2::NatGateway | 是 | 是 | 是 | 否 |
| AWS::EC2::NetworkAcl | 是 | 是 | 是 | 是 |
| AWS::EC2::NetworkInsightsAccessScope | 是 | 是 | 否 | 否 |
| AWS::EC2::NetworkInsightsAccessScope分析 | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EC2::NetworkInsights分析 | 是 | 是 | 否 | 否 |
| AWS::EC2::NetworkInsights路徑 | 是 | 是 | 否 | 否 |
| AWS::EC2::NetworkInterface | 是 | 是 | 是 | 是 |
| AWS::EC2::PrefixList | 是 | 是 | 是 | 是 |
| AWS::EC2::RouteTable | 是 | 是 | 是 | 是 |
| AWS::EC2::SecurityGroup | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EC2::SpotFleet | 是 | 是 | 是 | 是 |
| AWS::EC2::Subnet | 是 | 是 | 是 | 是 |
| AWS::EC2::SubnetRouteTableAssociation | 是 | 是 | 是 | 是 |
| AWS::EC2::TrafficMirror過濾器 | 是 | 否 | 否 | 否 |
| AWS::EC2::TrafficMirror階段 | 是 | 否 | 否 | 否 |
| AWS::EC2::TrafficMirror目標 | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EC2::TransitGateway | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGateway附件 | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGatewayConnect | 是 | 是 | 是 | 否 |
| AWS::EC2::TransitGatewayMulticastDomain | 是 | 是 | 是 | 是 |
| AWS::EC2::TransitGatewayRouteTable | 是 | 是 | 是 | 否 |
| AWS::EC2::VPC | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EC2::VPCEndpoint | 是 | 是 | 是 | 是 |
| AWS:: EC2:: VPC EndpointService | 是 | 是 | 是 | 是 |
| AWS:: EC2:: VPC PeeringConnection | 是 | 是 | 是 | 是 |
| AWS::EC2::VPNConnection | 是 | 是 | 是 | 是 |
| AWS::EC2::VPNGateway | 是 | 是 | 是 | 是 |
| AWS::EC2::Volume | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ECR::PullThroughCacheRule | 是 | 是 | 是 | 是 |
| AWS::ECR::RegistryPolicy | 是 | 是 | 是 | 否 |
| AWS::ECR::Repository | 是 | 是 | 是 | 否 |
| AWS::ECS::CapacityProvider | 是 | 是 | 是 | 是 |
| AWS::ECS::Cluster | 是 | 是 | 是 | 是 |
| AWS::ECS::Service | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ECS::TaskDefinition | 是 | 是 | 是 | 是 |
| AWS::ECS::TaskSet | 是 | 是 | 是 | 否 |
| AWS::EFS::AccessPoint | 是 | 是 | 是 | 否 |
| AWS::EFS::FileSystem | 是 | 是 | 是 | 否 |
| AWS::EKS::Addon | 是 | 是 | 是 | 否 |
| AWS::EKS::Cluster | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::EKS::FargateProfile | 是 | 是 | 是 | 是 |
| AWS::EKS::IdentityProviderConfig | 是 | 是 | 是 | 否 |
| AWS::EMR::SecurityConfiguration | 是 | 是 | 是 | 否 |
| AWS::ElasticBeanstalk::Application | 否 | 是 | 否 | 否 |
| AWS::ElasticBeanstalk::ApplicationVersion | 否 | 是 | 否 | 否 |
| AWS::ElasticBeanstalk::Environment | 否 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ElasticLoadBalancing::LoadBalancer | 是 | 是 | 是 | 是 |
| AWS::ElasticLoadBalancingV2::Listener | 是 | 是 | 否 | 否 |
| AWS::ElasticLoadBalancingV2::LoadBalancer | 是 | 是 | 是 | 是 |
| AWS::Elasticsearch::Domain | 是 | 是 | 是 | 是 |
| AWS::Events::ApiDestination | 是 | 是 | 否 | 否 |
| AWS::Events::Archive | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Events::Connection | 是 | 是 | 否 | 否 |
| AWS::Events::EventBus | 是 | 是 | 否 | 否 |
| AWS::Events::Rule | 是 | 是 | 否 | 否 |
| AWS::FIS::ExperimentTemplate | 是 | 是 | 否 | 否 |
| AWS::Glue::Classifier | 是 | 是 | 是 | 是 |
| AWS::Glue::Job | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Glue:: 毫升變換 | 是 | 是 | 是 | 是 |
| AWS::GroundStation::Config | 是 | 是 | 否 | 否 |
| AWS::GroundStation::DataflowEndpoint集團 | 是 | 是 | 否 | 否 |
| AWS::GroundStation::MissionProfile | 是 | 是 | 否 | 否 |
| AWS::GuardDuty::Detector | 是 | 是 | 否 | 否 |
| AWS::GuardDuty::Filter | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Guard責任:: 集 | 是 | 是 | 否 | 否 |
| AWS::GuardDuty::ThreatIntel套裝 | 是 | 是 | 否 | 否 |
| AWS::IAM::Group | 是 | 是 | 否 | 否 |
| AWS::IAM::Policy | 是 | 是 | 否 | 否 |
| AWS::IAM::Role | 是 | 是 | 否 | 否 |
| AWS::IAM::User | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ImageBuilder::ContainerRecipe | 是 | 是 | 是 | 是 |
| AWS::ImageBuilder::DistributionConfiguration | 是 | 是 | 否 | 否 |
| AWS::ImageBuilder::ImagePipeline | 是 | 是 | 是 | 是 |
| AWS::ImageBuilder::ImageRecipe | 是 | 是 | 否 | 否 |
| AWS::ImageBuilder::InfrastructureConfiguration | 是 | 是 | 是 | 是 |
| AWS::InspectorV2::Filter | 是 | 否 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::IoT::AccountAudit配置 | 是 | 否 | 是 | 否 |
| AWS::IoT::Authorizer | 是 | 否 | 是 | 否 |
| AWS::IoT:: 緩存 | 是 | 否 | 是 | 否 |
| AWS::IoT::CustomMetric | 是 | 否 | 是 | 否 |
| AWS::IoT::Dimension | 是 | 否 | 是 | 否 |
| AWS::IoT::FleetMetric | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::IoT::JobTemplate | 是 | 否 | 是 | 否 |
| AWS::IoT::MitigationAction | 是 | 否 | 是 | 否 |
| AWS::IoT::Policy | 是 | 否 | 是 | 否 |
| AWS::IoT::ProvisioningTemplate | 是 | 否 | 是 | 否 |
| AWS::IoT::RoleAlias | 是 | 否 | 是 | 否 |
| AWS::IoT::ScheduledAudit | 是 | 否 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::IoT::SecurityProfile | 是 | 否 | 是 | 否 |
| AWS::KMS::Alias | 是 | 是 | 否 | 否 |
| AWS::KMS::Key | 是 | 是 | 是 | 是 |
| AWS::Kinesis::Stream | 是 | 是 | 是 | 否 |
| AWS::Kinesis::StreamConsumer | 是 | 是 | 是 | 否 |
| AWS::KinesisAnalyticsV2::Application | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::KinesisFirehose::DeliveryStream | 是 | 是 | 是 | 是 |
| AWS::Lambda::CodeSigningConfig | 是 | 是 | 否 | 否 |
| AWS::Lambda::Function | 是 | 是 | 是 | 是 |
| AWS::Lex::Bot | 否 | 是 | 否 | 否 |
| AWS::Lex::BotAlias | 否 | 是 | 否 | 否 |
| AWS::Logs::Destination | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::MSK::BatchScram秘密 | 是 | 是 | 是 | 否 |
| AWS::MSK::Cluster | 是 | 是 | 是 | 否 |
| AWS::MSK::ClusterPolicy | 是 | 是 | 是 | 是 |
| AWS::MSK::Configuration | 是 | 是 | 是 | 否 |
| AWS::MSK::VpcConnection | 是 | 是 | 是 | 是 |
| AWS::MediaConnect::FlowEntitlement | 否 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::MediaConnect::FlowSource | 否 | 是 | 否 | 否 |
| AWS::MediaConnect::FlowVpc介面 | 否 | 是 | 否 | 否 |
| AWS::MediaTailor::PlaybackConfiguration | 否 | 是 | 否 | 否 |
| AWS::NetworkFirewall::Firewall | 是 | 是 | 是 | 是 |
| AWS::NetworkFirewall::FirewallPolicy | 是 | 是 | 是 | 是 |
| AWS::NetworkFirewall::RuleGroup | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Network防火牆:: TLS InspectionConfiguration | 是 | 是 | 是 | 是 |
| AWS::OpenSearch::Domain | 是 | 是 | 否 | 否 |
| AWS::RDS::DBCluster | 是 | 是 | 是 | 否 |
| AWS:: RDS:: 資料庫 ClusterSnapshot | 是 | 是 | 是 | 否 |
| AWS::RDS::DBInstance | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SecurityGroup | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::RDS::DBSnapshot | 是 | 是 | 是 | 是 |
| AWS:: RDS:: 資料庫 SubnetGroup | 是 | 是 | 是 | 是 |
| AWS::RDS::EventSubscription | 是 | 是 | 是 | 是 |
| AWS::RDS::OptionGroup | 是 | 是 | 是 | 否 |
| AWS::Redshift::Cluster | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterParameter集團 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Redshift::ClusterSecurity集團 | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSnapshot | 是 | 是 | 是 | 是 |
| AWS::Redshift::ClusterSubnet集團 | 是 | 是 | 是 | 是 |
| AWS::Redshift::EventSubscription | 是 | 是 | 是 | 是 |
| AWS::Redshift::ScheduledAction | 是 | 否 | 否 | 否 |
| AWS::ResilienceHub::App | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ResilienceHub::ResiliencyPolicy | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::FirewallDomain列表 | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::FirewallRule集團 | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::ResolverEndpoint | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::Route53Resolver::ResolverQueryLoggingConfig協會 | 是 | 是 | 否 | 否 |
| AWS::Route53Resolver::ResolverRule | 是 | 是 | 是 | 否 |
| AWS::Route53Resolver::ResolverRule協會 | 是 | 是 | 是 | 否 |
| AWS::S3::AccessPoint | 是 | 是 | 是 | 是 |
| AWS::S3::AccountPublicAccessBlock | 是 | 是 | 否 | 否 |
| AWS::S3::Bucket | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::SES::ConfigurationSet | 是 | 是 | 否 | 否 |
| AWS::SES::ContactList | 是 | 是 | 否 | 否 |
| AWS::SES::Template | 是 | 是 | 否 | 否 |
| AWS::SNS::Topic | 是 | 是 | 否 | 否 |
| AWS::SQS::Queue | 是 | 是 | 否 | 否 |
| AWS::SSM::AssociationCompliance | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::SSM::Document | 是 | 是 | 是 | 是 |
| AWS::SSM::FileData | 是 | 是 | 是 | 是 |
| AWS::SSM::ManagedInstance庫存 | 是 | 是 | 是 | 是 |
| AWS::SSM::PatchCompliance | 是 | 是 | 是 | 是 |
| AWS::SageMaker::AppImageConfig | 是 | 是 | 否 | 否 |
| AWS::SageMaker::CodeRepository | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::SageMaker::Domain | 是 | 是 | 否 | 否 |
| AWS::SageMaker::EndpointConfig | 是 | 是 | 否 | 否 |
| AWS::SageMaker::FeatureGroup | 是 | 是 | 否 | 否 |
| AWS::SageMaker::Image | 是 | 是 | 否 | 否 |
| AWS::SageMaker::Model | 是 | 是 | 否 | 否 |
| AWS::SageMaker::NotebookInstance | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::SageMaker::NotebookInstanceLifecycleConfig | 是 | 是 | 否 | 否 |
| AWS::SecretsManager::Secret | 是 | 是 | 是 | 是 |
| AWS::ServiceCatalog::CloudFormation产品 | 是 | 是 | 是 | 否 |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | 是 | 是 | 是 | 否 |
| AWS::ServiceCatalog::Portfolio | 是 | 是 | 是 | 否 |
| AWS::ServiceDiscovery::HttpNamespace | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::ServiceDiscovery::Instance | 是 | 是 | 是 | 否 |
| AWS::ServiceDiscovery::PublicDns命名空 | 是 | 是 | 是 | 否 |
| AWS::ServiceDiscovery::Service | 是 | 是 | 是 | 否 |
| AWS::ShieldRegional::Protection | 是 | 是 | 是 | 否 |
| AWS::Signer::SigningProfile | 是 | 是 | 否 | 否 |
| AWS::StepFunctions::Activity | 是 | 是 | 是 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::StepFunctions::StateMachine | 是 | 是 | 是 | 否 |
| AWS::Transfer::Agreement | 是 | 是 | 是 | 否 |
| AWS::Transfer::Certificate | 是 | 是 | 是 | 否 |
| AWS::Transfer::Connector | 是 | 是 | 是 | 否 |
| AWS::Transfer::Profile | 是 | 是 | 是 | 是 |
| AWS::Transfer::Workflow | 是 | 是 | 否 | 否 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::WAFRegional::RateBased規則 | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::Rule | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::RuleGroup | 是 | 是 | 是 | 是 |
| AWS::WAFRegional::WebACL | 是 | 是 | 是 | 是 |
| AWS::WAFv2::IPSet | 是 | 是 | 是 | 是 |
| AWS::WAFv2::ManagedRule套裝 | 是 | 是 | 是 | 是 |

| Resource Type (資源類型) | 非洲 (開普敦) | 中東 (巴林) | 中東 (阿拉伯聯合大公國) | 以色列 (特拉維夫) |
|---|---|---|---|---|
| AWS::WAFv2::RegexPattern套裝 | 是 | 是 | 是 | 是 |
| AWS::WAFv2::RuleGroup | 是 | 是 | 是 | 是 |
| AWS::WAFv2::WebACL | 是 | 是 | 是 | 是 |
| AWS::WorkSpaces::Workspace | 否 | 是 | 否 | 否 |
| AWS::XRay::EncryptionConfig | 否 | 是 | 是 | 是 |

# GovCloud 地區

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::ACM::Certificate | 是 | 是 |
| AWS::ACMPCA::CertificateAuthority | 是 | 是 |
| AWS::ACMPCA::CertificateAuthority激活 | 是 | 是 |
| AWS::AccessAnalyzer::Analyzer | 是 | 是 |
| AWS::AmazonMQ::Broker | 是 | 是 |
| AWS::ApiGateway::RestApi | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::ApiGateway::Stage | 是 | 是 |
| AWS::ApiGatewayV2::Api | 是 | 是 |
| AWS::ApiGatewayV2::Stage | 是 | 是 |
| AWS::AppConfig::Application | 是 | 是 |
| AWS::AppConfig::ConfigurationProfile | 是 | 是 |
| AWS::AppConfig::DeploymentStrategy | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::AppConfig::Environment | 是 | 是 |
| AWS::AppConfig::ExtensionAssociation | 是 | 是 |
| AWS::AppConfig::HostedConfiguration版本 | 是 | 是 |
| AWS::AppStream::Application | 是 | 是 |
| AWS::AppStream::DirectoryConfig | 否 | 是 |
| AWS::AppStream::Fleet | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::AppStream::Stack | 否 | 是 |
| AWS::Athena::DataCatalog | 是 | 是 |
| AWS::Athena::WorkGroup | 是 | 是 |
| AWS::AutoScaling::AutoScaling集團 | 是 | 是 |
| AWS::AutoScaling::LaunchConfiguration | 是 | 是 |
| AWS::AutoScaling::ScalingPolicy | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::AutoScaling::ScheduledAction | 是 | 是 |
| AWS::AutoScaling::WarmPool | 是 | 是 |
| AWS::Backup::BackupPlan | 是 | 是 |
| AWS::Backup::BackupSelection | 是 | 是 |
| AWS::Backup::BackupVault | 是 | 是 |
| AWS::Backup::RecoveryPoint | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::Batch::ComputeEnvironment | 是 | 是 |
| AWS::Batch::JobQueue | 是 | 是 |
| AWS::Batch::SchedulingPolicy | 是 | 是 |
| AWS::Cassandra::Keyspace | 是 | 是 |
| AWS::CloudFormation::Stack | 是 | 是 |
| AWS::CloudTrail::Trail | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::CloudWatch::Alarm | 是 | 是 |
| AWS::CodeBuild::Project | 是 | 是 |
| AWS::CodeBuild::ReportGroup | 是 | 是 |
| AWS::Cognito::UserPool集團 | 否 | 是 |
| AWS::Config::ConfigurationRecorder | 是 | 是 |
| AWS::Config::ConformancePack合規 | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::Config::ResourceCompliance | 是 | 是 |
| AWS::Connect::Instance | 否 | 是 |
| AWS::Connect::QuickConnect | 否 | 是 |
| AWS::DMS::Certificate | 是 | 是 |
| AWS::DMS::Endpoint | 是 | 是 |
| AWS::DMS::EventSubscription | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::DMS::ReplicationInstance | 是 | 是 |
| AWS::DMS::ReplicationSubnet集團 | 是 | 是 |
| AWS::DMS::ReplicationTask | 是 | 是 |
| AWS::DataSync::LocationEFS | 是 | 是 |
| AWS::DataSync::LocationF SxLustre | 是 | 是 |
| AWS::DataSync::LocationF SxWindows | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::DataSync::LocationHDFS | 是 | 是 |
| AWS::DataSync::LocationNFS | 是 | 是 |
| AWS::DataSync::LocationObject儲存 | 是 | 是 |
| AWS::DataSync::LocationS3 | 是 | 是 |
| AWS::DataSync::Location中小企 | 是 | 是 |
| AWS::DataSync::Task | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::Detective::Graph | 是 | 是 |
| AWS::DynamoDB::Table | 是 | 是 |
| AWS::EC2::CapacityReservation | 是 | 是 |
| AWS::EC2::ClientVpn端點 | 是 | 是 |
| AWS::EC2::CustomerGateway | 是 | 是 |
| AWS::EC2::DHCPOptions | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::EC2::EC2Fleet | 是 | 是 |
| AWS::EC2::EIP | 是 | 是 |
| AWS::EC2::EgressOnlyInternetGateway | 是 | 是 |
| AWS::EC2::FlowLog | 是 | 是 |
| AWS::EC2::Host | 是 | 是 |
| AWS::EC2::IPAM | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::EC2::IPAMPool | 是 | 是 |
| AWS::EC2::IPAMScope | 是 | 是 |
| AWS::EC2::Instance | 是 | 是 |
| AWS::EC2::InternetGateway | 是 | 是 |
| AWS::EC2::LaunchTemplate | 是 | 是 |
| AWS::EC2::NatGateway | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::EC2::NetworkAcl | 是 | 是 |
| AWS::EC2::NetworkInterface | 是 | 是 |
| AWS::EC2::PrefixList | 是 | 是 |
| AWS::EC2::RouteTable | 是 | 是 |
| AWS::EC2::SecurityGroup | 是 | 是 |
| AWS::EC2::SpotFleet | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::EC2::Subnet | 是 | 是 |
| AWS::EC2::SubnetRouteTableAssociation | 是 | 是 |
| AWS::EC2::TrafficMirror過濾器 | 是 | 是 |
| AWS::EC2::TrafficMirror階段 | 是 | 是 |
| AWS::EC2::TrafficMirror目標 | 是 | 是 |
| AWS::EC2::TransitGateway | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::EC2::TransitGateway附件 | 是 | 是 |
| AWS::EC2::TransitGatewayConnect | 是 | 是 |
| AWS::EC2::TransitGatewayMulticastDomain | 是 | 是 |
| AWS::EC2::TransitGatewayRouteTable | 是 | 是 |
| AWS::EC2::VPC | 是 | 是 |
| AWS::EC2::VPCEndpoint | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS:: EC2:: VPC EndpointService | 否 | 是 |
| AWS:: EC2:: VPC PeeringConnection | 是 | 是 |
| AWS::EC2::VPNConnection | 是 | 是 |
| AWS::EC2::VPNGateway | 是 | 是 |
| AWS::EC2::Volume | 是 | 是 |
| AWS::ECR::Repository | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::ECS::CapacityProvider | 是 | 是 |
| AWS::ECS::Cluster | 是 | 是 |
| AWS::ECS::Service | 是 | 是 |
| AWS::ECS::TaskDefinition | 是 | 是 |
| AWS::ECS::TaskSet | 是 | 是 |
| AWS::EFS::AccessPoint | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::EFS::FileSystem | 是 | 是 |
| AWS::EKS::Addon | 是 | 是 |
| AWS::EKS::Cluster | 是 | 是 |
| AWS::EKS::IdentityProviderConfig | 是 | 是 |
| AWS::EMR::SecurityConfiguration | 是 | 是 |
| AWS::ElasticBeanstalk::Application | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::ElasticBeanstalk::ApplicationVersion | 是 | 是 |
| AWS::ElasticBeanstalk::Environment | 是 | 是 |
| AWS::ElasticLoadBalancing::LoadBalancer | 是 | 是 |
| AWS::ElasticLoadBalancingV2::Listener | 是 | 是 |
| AWS::ElasticLoadBalancingV2::LoadBalancer | 是 | 是 |
| AWS::Elasticsearch::Domain | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::Events::EventBus | 是 | 是 |
| AWS::Events::Rule | 是 | 是 |
| AWS::FIS::ExperimentTemplate | 是 | 是 |
| AWS::Glue::Classifier | 是 | 是 |
| AWS::Glue::Job | 是 | 是 |
| AWS::Glue:: 毫升變換 | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::GreengrassV2::ComponentVersion | 是 | 是 |
| AWS::GuardDuty::Detector | 是 | 是 |
| AWS::GuardDuty::Filter | 是 | 是 |
| AWS::Guard責任:: 集 | 是 | 是 |
| AWS::GuardDuty::ThreatIntel套裝 | 是 | 是 |
| AWS::IAM::Group | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::IAM::InstanceProfile | 是 | 否 |
| AWS::IAM::OIDCProvider | 是 | 否 |
| AWS::IAM::Policy | 是 | 是 |
| AWS::IAM::Role | 是 | 是 |
| AWS::IAM::SAMLProvider | 是 | 否 |
| AWS::IAM::ServerCertificate | 是 | 否 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::IAM::User | 是 | 是 |
| AWS::ImageBuilder::ContainerRecipe | 是 | 是 |
| AWS::ImageBuilder::DistributionConfiguration | 是 | 是 |
| AWS::ImageBuilder::ImagePipeline | 是 | 是 |
| AWS::ImageBuilder::ImageRecipe | 是 | 是 |
| AWS::ImageBuilder::InfrastructureConfiguration | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::IoT::AccountAudit配置 | 是 | 是 |
| AWS::IoT::Authorizer | 是 | 是 |
| AWS::IoT:: 緩存 | 是 | 是 |
| AWS::IoT::CustomMetric | 是 | 是 |
| AWS::IoT::Dimension | 是 | 是 |
| AWS::IoT::FleetMetric | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::IoT::JobTemplate | 是 | 是 |
| AWS::IoT::MitigationAction | 是 | 是 |
| AWS::IoT::Policy | 是 | 是 |
| AWS::IoT::ProvisioningTemplate | 是 | 是 |
| AWS::IoT::RoleAlias | 是 | 是 |
| AWS::IoT::ScheduledAudit | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::IoT::SecurityProfile | 是 | 是 |
| AWS::IoTEvents::AlarmModel | 否 | 是 |
| AWS::IoTEvents::DetectorModel | 否 | 是 |
| AWS::IoTEvents::Input | 否 | 是 |
| AWS::IoTSiteWise::AssetModel | 否 | 是 |
| AWS::IoTSiteWise::Gateway | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::IoTSiteWise::Portal | 否 | 是 |
| AWS::IoTTwinMaker::ComponentType | 否 | 是 |
| AWS::IoTTwinMaker::Entity | 否 | 是 |
| AWS::IoTTwinMaker::Workspace | 否 | 是 |
| AWS::KMS::Alias | 是 | 是 |
| AWS::KMS::Key | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::Kinesis::Stream | 是 | 是 |
| AWS::Kinesis::StreamConsumer | 是 | 是 |
| AWS::KinesisAnalyticsV2::Application | 是 | 是 |
| AWS::KinesisFirehose::DeliveryStream | 是 | 是 |
| AWS::Lambda::Function | 是 | 是 |
| AWS::Logs::Destination | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::MSK::BatchScram秘密 | 是 | 是 |
| AWS::MSK::Cluster | 是 | 是 |
| AWS::MSK::ClusterPolicy | 是 | 是 |
| AWS::MSK::Configuration | 是 | 是 |
| AWS::MSK::VpcConnection | 是 | 是 |
| AWS::NetworkFirewall::Firewall | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::NetworkFirewall::FirewallPolicy | 是 | 是 |
| AWS::NetworkFirewall::RuleGroup | 是 | 是 |
| AWS::NetworkManager::CustomerGateway協會 | 否 | 是 |
| AWS::NetworkManager::Device | 否 | 是 |
| AWS::NetworkManager::GlobalNetwork | 否 | 是 |
| AWS::NetworkManager::Link | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::NetworkManager::LinkAssociation | 否 | 是 |
| AWS::NetworkManager::Site | 否 | 是 |
| AWS::NetworkManager::TransitGateway注册 | 否 | 是 |
| AWS::OpenSearch::Domain | 是 | 是 |
| AWS::Pinpoint::App | 否 | 是 |
| AWS::Pinpoint::ApplicationSettings | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::Pinpoint::Campaign | 否 | 是 |
| AWS::Pinpoint::EmailChannel | 否 | 是 |
| AWS::Pinpoint::EmailTemplate | 否 | 是 |
| AWS::Pinpoint::EventStream | 否 | 是 |
| AWS::Pinpoint::InApp。模板 | 否 | 是 |
| AWS::Pinpoint::Segment | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::QuickSight::Template | 否 | 是 |
| AWS::RDS::DBCluster | 是 | 是 |
| AWS:: RDS:: 資料庫 ClusterSnapshot | 是 | 是 |
| AWS::RDS::DBInstance | 是 | 是 |
| AWS:: RDS:: 資料庫 SecurityGroup | 是 | 是 |
| AWS::RDS::DBSnapshot | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS:: RDS:: 資料庫 SubnetGroup | 是 | 是 |
| AWS::RDS::EventSubscription | 是 | 是 |
| AWS::RDS::OptionGroup | 是 | 是 |
| AWS::Redshift::Cluster | 是 | 是 |
| AWS::Redshift::ClusterParameter集團 | 是 | 是 |
| AWS::Redshift::ClusterSecurity集團 | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
|---|---|---|
| AWS::Redshift::ClusterSnapshot | 是 | 是 |
| AWS::Redshift::ClusterSubnet集團 | 是 | 是 |
| AWS::Redshift::EventSubscription | 是 | 是 |
| AWS::Redshift::ScheduledAction | 是 | 是 |
| AWS::RoboMaker::RobotApplication | 否 | 是 |
| AWS::RoboMaker::RobotApplication版本 | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::RoboMaker::SimulationApplication | 否 | 是 |
| AWS::Route53Resolver::FirewallDomain列表 | 是 | 是 |
| AWS::Route53Resolver::FirewallRule集團 | 是 | 是 |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | 是 | 是 |
| AWS::Route53Resolver::ResolverEndpoint | 是 | 是 |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::Route53Resolver::ResolverQueryLoggingConfig協會 | 是 | 是 |
| AWS::Route53Resolver::ResolverRule | 是 | 是 |
| AWS::Route53Resolver::ResolverRule協會 | 是 | 是 |
| AWS::S3::AccessPoint | 是 | 是 |
| AWS::S3::AccountPublicAccessBlock | 是 | 是 |
| AWS::S3::Bucket | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::SES::ConfigurationSet | 否 | 是 |
| AWS::SES::ContactList | 否 | 是 |
| AWS::SES::Template | 否 | 是 |
| AWS::SNS::Topic | 是 | 是 |
| AWS::SQS::Queue | 是 | 是 |
| AWS::SSM::AssociationCompliance | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::SSM::Document | 是 | 是 |
| AWS::SSM::FileData | 是 | 是 |
| AWS::SSM::ManagedInstance庫存 | 是 | 是 |
| AWS::SSM::PatchCompliance | 是 | 是 |
| AWS::SageMaker::Model | 否 | 是 |
| AWS::SageMaker::NotebookInstance | 否 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | 否 | 是 |
| AWS::SecretsManager::Secret | 是 | 是 |
| AWS::ServiceCatalog::CloudFormation产品 | 是 | 是 |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | 是 | 是 |
| AWS::ServiceCatalog::Portfolio | 是 | 是 |
| AWS::ServiceDiscovery::HttpNamespace | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::ServiceDiscovery::Instance | 是 | 是 |
| AWS::ServiceDiscovery::Service | 是 | 是 |
| AWS::StepFunctions::StateMachine | 是 | 是 |
| AWS::Transfer::Agreement | 是 | 是 |
| AWS::Transfer::Certificate | 是 | 是 |
| AWS::Transfer::Connector | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::Transfer::Profile | 是 | 是 |
| AWS::Transfer::Workflow | 是 | 是 |
| AWS::WAFRegional::RateBased規則 | 是 | 是 |
| AWS::WAFRegional::Rule | 是 | 是 |
| AWS::WAFRegional::RuleGroup | 是 | 是 |
| AWS::WAFRegional::WebACL | 是 | 是 |

| Resource Type (資源類型) | AWS GovCloud (美國西部) | AWS GovCloud (美國東部) |
| --- | --- | --- |
| AWS::WAFv2::IPSet | 是 | 是 |
| AWS::WAFv2::ManagedRule套裝 | 是 | 是 |
| AWS::WAFv2::RegexPattern套裝 | 是 | 是 |
| AWS::WAFv2::RuleGroup | 是 | 是 |
| AWS::WAFv2::WebACL | 是 | 是 |
| AWS::WorkSpaces::Workspace | 否 | 是 |

# 錄製 AWS 資源

AWS Config 持續偵測何時建立、變更或刪除支援的資源類型。 AWS Config 將這些事件記錄為組態項目 (CI)。您可以自訂 AWS Config 來記錄所有支援資源類型的組態變更，或記錄僅與您相關之資源類型的組態變更。如需可 AWS Config 以記錄的受支援資源類型清單，請參閱支援的資源類型。

## 考量事項

大量的 AWS Config 評估

與後續月份相比，您可能會注意到在使用 AWS Config 錄製的初始月份期間，帳戶中的活動有所增加。在初始啟動安裝程序期間， AWS Config 會對 AWS Config 您帳戶中選取要記錄的所有資源執行評估。

如果您正在執行暫時工作負載，您可能會看到活動增加， AWS Config 因為它會記錄與建立和刪除這些暫時資源相關聯的組態變更。暫時性工作負載是暫時使用因需要而載入和執行的運算資源。範例包括 Amazon Elastic Compute Cloud (Amazon EC2) Spot 執行個體、Amazon EMR 作業和 AWS Auto Scaling。如果您想要避免因執行臨時工作負載而增加的活動，您可以設定組態錄製程式以將這些資源類型排除在記錄之外，或在關 AWS Config 閉的情況下在單獨的帳戶中執行這些類型的工作負載，以避免增加組態記錄和規則評估。

區域可用性

在指定 AWS Config 要追蹤的資源型態之前，請先勾選「依區域」的可用性「資源涵蓋範圍」，以查看您設定的「 AWS 區域」中是否支援資源型態 AWS Config。如果至少一個「區域」支援某個資源類型，則您可以 AWS Config 在所支援的所有「區域」中啟用該資源類型的記錄 AWS Config，即使您設定的「 AWS 區域」不支援指定的資源類型也一樣 AWS Config。

## 區域資源和全球資源有何不同？

區域資源

區域資源與區域繫結，且僅能在該區域中使用。您可以在指定的中創建它們 AWS 區域，然後它們存在於該區域中。若要查看這些資源或與其互動，您必須將操作導向至該區域。例如，若要使用建立 Amazon EC2 執行個體 AWS Management Console，您可以選擇要在 AWS 區域其中建立執行個體的執行個體。如果使用 AWS Command Line Interface (AWS CLI) 建立例證，則包括`--region`參數。每個 AWS SDK 都有自己的等效機制來指定操作使用的區域。

使用區域資源的原因有幾個。其中一個原因是要確保資源及您用來存取這些資源的服務端點盡可能靠近客戶。這可將延遲降至最低來提高效能。另一個原因是要提供隔離界限。這可讓您在多個區域中建立獨立的資源副本，以分發負載並改善可擴展性。同時，其可將資源彼此隔離以提高可用性。

如果您在控制台或 AWS CLI 命令 AWS 區域 中指定了不同的資源，則您將無法再查看或與之前「區域」中可以看到的資源進行交互。

當您查看區域資源的《Amazon Resource Name (ARN)》時，會將包含資源的區域指定為 ARN 中的第四個欄位。例如，Amazon EC2 執行個體是區域資源。以下是 `us-east-1` 區域中存在之 Amazon EC2 執行個體的 ARN 範例。

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

全域資源

某些 AWS 服務資源是全球資源，這意味著您可以從任何地方使用資源。您不會在全域服務的主控台中指定 AWS 區域 。若要存取全域資源，請勿在使用服務 AWS CLI 和 AWS SDK 作業時指定`--region`參數。

全域資源支援一次只能存在一個特定資源執行個體此一關鍵情況。在這些情境下，在不同區域副本之間進行複寫或同步處理並不足夠。必須存取單一全域端點 (但可能會增加延遲) 是可接受的考量，以確保資源的消費者可立即看到任何變更。

例如，Amazon Aurora 全域叢集 (`AWS::RDS::GlobalCluster`) 是全域資源，因此不會與區域繫結。這表示您可以建立全域叢集，而不需仰賴區域端點。好處是，雖然 Amazon Relational Database Service (Amazon RDS) 本身是依區域組織的，但全域叢集來源的特定區域不會影響全域叢集。其會顯示為跨所有區域的單一連續全域叢集。

全域資源的《Amazon Resource Name (ARN)》不包含區域。第四個欄位為空白，例如以下全域叢集的 ARN 範例中。

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> 在 2022 年 2 月 AWS Config 之後登入的全域資源類型，只會記錄在服務的商業區域和分割區的 AWS GovCloud (美國西部)。 GovCloud 您只能在其本地區域和 (美國西部) 檢視這些新全域資源類型的組態項目 AWS GovCloud (CI)。
> 在 2022 年 2 月之前上線的全域資源類型 (`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role` 和 `AWS::IAM::User`) 保持不變。您可以在 2022 年 2 月之前獲 AWS Config 得支援的所有區域啟用這些全球 IAM 資源的記錄功能。這些全球 IAM 資源無法在 2022 年 2 月 AWS Config 之後支援的區域中記錄。

全域資源類型 | IAM 資源

下列 IAM 資源類型為全域記錄：IAM 使用者、群組、角色和客戶管理政策。這些資源類型可以 AWS Config 在 2022 年 2 月之前提供的區域中記錄。 AWS Config 如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

若要避免重複的設定項目 (CI)，您應該考慮只在其中一個支援的區域中記錄全域 IAM 資源類型一次。這也可協助您避免不必要的評估和 API 限流。

全域資源類型 | 僅限主要區域

以下服務的全球資源僅 AWS Config 在全球資源類型的本地區域中記錄：Amazon 彈性容器註冊表公共 AWS Global Accelerator，Amazon 路線 53 CloudFront，Amazon 和 AWS WAF. 對於這些全域資源，資源類型的相同執行個體可以在多個區 AWS 域中使用，但組態項目 (CI) 只會記錄在商業分割區的本位目錄區域，或記錄在分割區的 AWS GovCloud (美國西部)。 AWS GovCloud (US)

全域資源類型的主要區域

| AWS 服務 | 資源類型值 | 主要區域 |
| --- | --- | --- |
| Amazon Elastic Container Registry Public | `AWS::ECR::PublicRepository` | 美國東部 (維吉尼亞北部) 區域 |
| AWS Global Accelerator | `AWS::GlobalAccelerator::Listener` | 美國西部 (奧勒岡) 區域 |
| | `AWS::GlobalAccelerator::EndpointGroup` | 美國西部 (奧勒岡) 區域 |
| | `AWS::GlobalAccelerator::Accelerator` | 美國西部 (奧勒岡) 區域 |
| Amazon Route 53 | `AWS::Route53::HostedZone` | 美國東部 (維吉尼亞北部) 區域 |
| | `AWS::Route53::HealthCheck` | 美國東部 (維吉尼亞北部) 區域 |

| AWS 服務 | 資源類型值 | 主要區域 |
| --- | --- | --- |
| Amazon CloudFront | `AWS::CloudFront::Distribution` | 美國東部 (維吉尼亞北部) 區域 |
| AWS WAF | `AWS::WAFv2::WebACL` | 美國東部 (維吉尼亞北部) 區域 |

全域資源類型 | Aurora 全域叢集

`AWS::RDS::GlobalCluster`是在啟用組態記錄程式的所有受支援 AWS Config 區域中記錄的全域資源。此全域資源類型是唯一的，因為如果您在一個區域中啟用此資源的記錄，則 AWS Config 會在所有已啟用的區域中記錄此資源類型的組態項目 (CI)。

如果您不想`AWS::RDS::GlobalCluster`在所有已啟用的區域中進行錄製，請針對 AWS Config 主控台使用下列其中一種錄製策略：

- 使用可自定義的覆蓋記錄所有資源類型，選擇 GlobalCluster「AWS RDS」，然後選擇覆蓋「從錄製中排除」
- 記錄特定資源類型。

如果您不想要在所有已啟用的區域中記錄 `AWS::RDS::GlobalCluster`，請針對 API/CLI 使用下列一種記錄策略：

- 記錄所有目前和未來的資源類型 (包括排除項目) (`EXCLUSION_BY_RESOURCE_TYPES`)
- 記錄特定資源類型 (`INCLUSION_BY_RESOURCE_TYPES`)。

## 在 AWS Config 主控台中錄製資源

記錄資源（主控台）

您可以使用 AWS Config 主控台來選取 AWS Config 記錄的資源類型。

選取資源

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在左側導覽窗格中，選擇設定，然後選擇編輯。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 端點和配額。

3. 在記錄方法區段中，選擇記錄策略。您可以指定要 AWS Config 記錄的 AWS 資源。

   All resource types with customizable overrides

   設定 AWS Config 以記錄此區域中所有目前與 future 支援之資源型態的組態變更。您可以覆寫特定資源類型的記錄頻率，或從記錄中排除特定資源類型。如需詳細資訊，請參閱《支援的資源類型》。

   - 預設設定

     為所有目前和未來支援的資源類型設定預設記錄頻率。如需詳細資訊，請參閱記錄頻率。

     - 連續錄製 — 每當發生變更時，都 AWS Config 會持續記錄組態變更。
     - 每日記錄 – 您可接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。

     > **Note**
     > AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

   - 覆寫設定

     覆寫特定資源類型的記錄頻率，或從記錄中排除特定資源類型。如果您變更某資源類型的記錄頻率，則已記錄的組態項目會保持不變。

     > **Note**
     > 全域資源類型 | Aurora 全域叢集最初包含在記錄中
     > 資`AWS::RDS::GlobalCluster`源類型將記錄在啟用配置記錄器的所有支援 AWS Config 區域中。
     > 如果您不想在所有已啟用的區域中記錄 `AWS::RDS::GlobalCluster`，請選擇「AWS RDS GlobalCluster」，然後選擇覆寫「從記錄中排除」。

     > **Note**
     > 全域資源類型 | IAM 資源類型最初會從記錄中排除

「所有全域記錄的 IAM 資源類型」最初會從記錄中排除，以協助您降低成本。此配套包含 IAM 使用者、群組、角色和客戶管理政策。選擇移除以移除覆寫，並將這些資源包含在您的記錄中。
此附註不涵蓋美國東部 (維吉尼亞北部)。全域 IAM 資源類型最初包含在美國東部 (維吉尼亞北部) 區域，因為該區域充當全球 IAM 資源類型的主區域。
此外，在 2022 年 2 月 AWS Config 之後支援的區域中 `AWS::IAM::User` `AWS::IAM::Group``AWS::IAM::Role`，無法記錄全域 IAM 資源類型 (、、和`AWS::IAM::Policy`)。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

> **Note**
>
> 限制
>
> 您最多可以增加到 100 個頻率覆寫及 600 個排除覆寫。
>
> 下列資源類型不支援每日記錄：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Specific resource types

設 AWS Config 定為僅記錄您指定之資源類型的組態變更。

- 特定資源類型

  選擇要記錄的資源類型及其頻率。如需詳細資訊，請參閱記錄頻率。

  - 連續錄製 — 每當發生變更時，都 AWS Config 會持續記錄組態變更。
  - 每日記錄 – 您可接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。

> **Note**
>
> AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

如果您變更某資源類型的記錄頻率，則已記錄的組態項目會保持不變。

> **Note**
>
> 區域可用性
>
> 在指定 AWS Config 要追蹤的資源型態之前，請先勾選「依區域」的可用性「資源涵蓋範圍」，以查看您設定的「 AWS 區域」中是否支援資源型態 AWS Config。如果至少一個「區域」支援某個資源類型，則您可以 AWS Config 在所支援的所有「區域」中啟用該資源類型的記錄 AWS Config，即使您設定的「 AWS 區域」不支援指定的資源類型也一樣 AWS Config。

> **Note**
>
> 限制
>
> 如果所有資源類型具有相同頻率，則無限制。如果至少有一種資源類型設定為「持續」，您最多可以使用「每日」頻率增加 100 個資源類型。
>
> 以下資源類型不支援每日頻率：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

4. 選擇儲存，以儲存變更。

## 使用 AWS CLI 記錄資源

### 錄製AWS CLI 資源

您可以使用 AWS CLI 選取要 AWS Config 記錄的資源類型。您可以透過建立組態記錄器來執行此作業，記錄您在記錄群組中指定的資源類型。在記錄群組中，您需要指定是要記錄所有支援的資源類型，還是包含或排除特定的資源類型。

Record all current and future supported resource types

設定 AWS Config 以記錄此區域中所有目前與 future 支援之資源型態的組態變更。如需詳細資訊，請參閱《支援的資源類型》。

1. 使用下列 put-configuration-recorder 命令：

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

此指令會使用`--configuration-recorder`和`---recording-group`欄位。

> **Note**
>
> 錄音組和配置記錄器
> `--recording-group` 欄位指定記錄的資源類型。
> 此`--configuration-recorder`欄位會指定name組態錄製程式的預設錄製頻率，以及 (`recordingMode`)。`roleArn`您也可以使用此欄位覆寫特定資源類型的記錄頻率。

i. put-configuration-recorder 會使用下列用於 `--recording-group` 參數的欄位：

- `allSupported=true`— AWS Config 記錄所有支援資源類型的組態變更，不包括全域 IAM 資源類型。新 AWS Config 增對新資源類型的支援時，會自動 AWS Config 開始記錄該類型的資源。
- `includeGlobalResourceTypes=true` – 此選項為搭售方案，僅適用於全域的 IAM 資源類型：IAM 使用者、群組、角色和客戶管理政策。這些全球 IAM 資源類型只能在 2022 年 2 月之前提供的 AWS Config 區域 AWS Config 中進行記錄。您無法在 2022 年 2 月 AWS Config 之後支援的區域中記錄全球 IAM 資源類型。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

> **Important**
>
> Aurora 全域叢集會記錄在所有啟用的區域中
> 資`AWS::RDS::GlobalCluster`源類型將記錄在啟用組態記錄程式的所有支援 AWS Config 區域中，即使未設定為也`includeGlobalResourceTypes`是如此`true`。此 `includeGlobalResourceTypes` 選項是僅適用於 IAM 使用者、群組、角色和客戶管理政策的配套。

如果不希望在所有已啟用的區域中記錄 AWS::RDS::GlobalCluster，請使用下列一種記錄策略：

1. 記錄所有目前和未來的資源類型，您指定的類型除外 (EXCLUSION_BY_RESOURCE_TYPES)，或
2. 記錄特定資源類型 (INCLUSION_BY_RESOURCE_TYPES)。

如需詳細資訊，請參閱選取要記錄的資源 | 區域和全域資源。

**Important**

包括GlobalResourceTypes 和排除記錄策略
該includeGlobalResourceTypes字段
對EXCLUSION_BY_RESOURCE_TYPES記錄策略沒有影響。這表示exclusionByResourceTypes當includeGlobalResourceTypes設為時，將不會自動新增全域 IAM 資源類型 (IAM 使用者、群組、角色和客戶受管政策) 做為排除項目false。
此includeGlobalResourceTypes欄位只應用於修改AllSupported欄位，因為欄位的預設值是記錄所有受支援資源類型 (不包括全AllSupported域 IAM 資源類型) 的組態變更。若要在設定為時AllSupported包含全域 IAM 資源類型true，請務必將設定includeGlobalResourceTypes為true。
若要排除EXCLUSION_BY_RESOURCE_TYPES記錄策略的全域 IAM 資源類型，您需要手動將它們新增到的resourceTypes欄位exclusionByResourceTypes。

**Note**

必要欄位和選用欄位
在將 includeGlobalResourceTypes 設定為 true 之前，請先將 allSupported 欄位設定為 true。
或者，也可以將 RecordingStrategy 的 useOnly 欄位設定為 ALL_SUPPORTED_RESOURCE_TYPES。

> **Note**
>
> 覆寫欄位
>
> 如果在的欄位中設定`includeGlobalResourceTypes`為`false`但列出全域 IAM 資源類型 RecordingGroup，則無論您是否 AWS Config 將`resourceTypes`欄位設定為 false，仍會記錄這些指定資源類型的`includeGlobalResourceTypes`組態變更。
>
> 如果您不想記錄全域 IAM 資源類型 (IAM 使用者、群組、角色和客戶管理政策) 的組態變更，除了將 `includeGlobalResourceTypes` 欄位設定為 false 之外，請切勿在 `resourceTypes` 欄位中列出這些類型。

`recordingGroup.json` 檔案可指定 AWS Config 記錄的資源類型。

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

ii. `put-configuration-recorder` 會使用下列用於 `--configuration-recorder` 參數的欄位：

- `name`— 組態記錄程式的名稱。 AWS Config 建立組態記錄器時，會自動指定「default」的名稱。
- `roleARN`— 由組態記錄器承擔 AWS Config 並使用之 IAM 角色的 Amazon 資源名稱 (ARN)。
- `recordingMode`— 指定用來記錄組態變更的預設錄製頻率。 AWS Config AWS Config 支持連續錄製和每日錄製。連續記錄可讓您在發生變更時持續記錄組態變更。每日記錄可讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。
  - `recordingFrequency`— AWS Config 用來記錄組態變更的預設錄製頻率。

> **Note**
>
> AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

- `recordingModeOverrides` — 此欄位可讓您指定記錄模式的覆寫。其為 `recordingModeOverride` 物件的陣列。`recordingModeOverrides` 陣列中的每個 `recordingModeOverride` 物件都包含三個欄位：
  - `description` — 您為覆寫提供的描述。
  - `recordingFrequency` — 會套用至覆寫中指定的所有資源類型的記錄頻率。
  - `resourceTypes`— 逗號分隔清單，指定覆寫中 AWS Config 包含哪些資源類型。

> **Note**
>
> 必要欄位和選用欄位
>
> put-configuration-recorder 的 `recordingMode` 欄位為選用。依預設，組態記錄器的記錄頻率設定為連續記錄。

> **Note**
>
> 限制
>
> 下列資源類型不支援每日記錄：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> 對於記錄所有目前和未來支援的資源類型 (`ALL_SUPPORTED_RESOURCE_TYPES`) 記錄策略，這些資源類型會設定為「連續記錄」。

`configurationRecorder.json`檔案會指定`name`組態錄製程式的預設錄製頻率，以及 (`recordingMode`)。`roleArn`您也可以使用此欄位覆寫特定資源類型的記錄頻率。

```
{
  "name": "default",
```

```
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (選擇性) 若要確認您的組態記錄器已具備所需設定，請使用下列《describe-configuration-recorders》命令。

```
$ aws configservice describe-configuration-recorders
```

以下是回應範例。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
```

```
                    "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

設定 AWS Config 為記錄所有目前和 future 支援的資源類型 (包括全域資源類型) 的組態變更，但您指定要從記錄中排除的資源類型除外。如果您選擇停止記錄某個資源類型，則已記錄的組態項目會保持不變。如需詳細資訊，請參閱《支援的資源類型》。

此指令會使用`--configuration-recorder`和`---recording-group`欄位。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> 錄音組和配置記錄器
> `--recording-group` 欄位指定記錄的資源類型。
> 此`--configuration-recorder`欄位會指定name組態錄製程式的預設錄製頻率，以及(`recordingMode`)。`roleArn`您也可以使用此欄位覆寫特定資源類型的記錄頻率。

1. 使用 `put-configuration-recorder` 命令，並在 `exclusionByResourceTypes` 的 `resourceTypes` 欄位中傳遞一或多個要排除的資源類型，如下列範例所示。
   i. `recordingGroup.json` 檔案可指定 AWS Config 記錄的資源類型。

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
```

```
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

指定要在記錄中排除的資源類型之前：

- 您必須將 `--recording-group` 參數的 `allSupported` 和 `includeGlobalResourceTypes` 欄位設定為 `false`，或予以省略。
- 您必須將 `RecordingStrategy` 的 `useOnly` 欄位設定為 `EXCLUSION_BY_RESOURCE_TYPES`。

> **Note**
>
> 覆寫欄位
>
> 如果記錄策略選擇 `EXCLUSION_BY_RESOURCE_TYPES`，則 `exclusionByResourceTypes` 欄位會覆寫請求中的其他屬性。
>
> 例如，除非您在 `exclusionByResourceTypes` 的 `resourceTypes` 欄位中特別將全域 IAM 資源類型列為排除項目，否則即使將 `includeGlobalResourceTypes` 設為 false，此選項仍會自動記錄這些資源類型。

> **Note**
>
> 全域資源類型和資源排除記錄策略
>
> 依預設，如果您選擇`EXCLUSION_BY_RESOURCE_TYPES`記錄策略，則當您在設定組態記錄程式的區域 (包括全域資源類型) 中新 AWS Config 增對新資源類型的支援時，會自動 AWS Config 開始記錄該類型的資源。
>
> 除非特別列為排除項目，否則在啟用組態記錄程式後，所有支援的 AWS Config 區域都`AWS::RDS::GlobalCluster`會自動記錄。
>
> IAM 使用者、群組、角色和客戶受管政策會記錄在您設定組態記錄器的區域 (如果該區域是 2022 年 2 月之前提供服務的區域)。 AWS Config 您無法在 2022 年 2 月

AWS Config 之後支援的區域中記錄全球 IAM 資源類型。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

ii. put-configuration-recorder 會使用下列用於 `--configuration-recorder` 參數的欄位：

- `name`— 組態記錄程式的名稱。 AWS Config 建立組態記錄器時，會自動指定「default」的名稱。
- `roleARN`— 由組態記錄器承擔 AWS Config 並使用之 IAM 角色的 Amazon 資源名稱 (ARN)。
- `recordingMode`— 指定用來記錄組態變更的預設錄製頻率。 AWS Config AWS Config 支持連續錄製和每日錄製。連續記錄可讓您在發生變更時持續記錄組態變更。每日記錄可讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。
  - `recordingFrequency`— AWS Config 用來記錄組態變更的預設錄製頻率。

    > **Note**
    > AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

  - `recordingModeOverrides` — 此欄位可讓您指定記錄模式的覆寫。其為 `recordingModeOverride` 物件的陣列。`recordingModeOverrides` 陣列中的每個 `recordingModeOverride` 物件都包含三個欄位：
    - `description` — 您為覆寫提供的描述。
    - `recordingFrequency` — 會套用至覆寫中指定的所有資源類型的記錄頻率。
    - `resourceTypes`— 逗號分隔清單，指定覆寫中 AWS Config 包含哪些資源類型。

> **Note**
> 必要欄位和選用欄位
> put-configuration-recorder 的 `recordingMode` 欄位為選用。依預設，組態記錄器的記錄頻率設定為連續記錄。

> **Note**
>
> 限制
>
> 下列資源類型不支援每日記錄：
>
> - AWS::Config::ResourceCompliance
> - AWS::Config::ConformancePackCompliance
> - AWS::Config::ConfigurationRecorder
>
> 對於記錄所有目前和未來支援的資源類型 (ALL_SUPPORTED_RESOURCE_TYPES) 記錄策略，這些資源類型會設定為「連續記錄」。

configurationRecorder.json檔案會指定name組態錄製程式的預設錄製頻率，以及(recordingMode)。roleArn您也可以使用此欄位覆寫特定資源類型的記錄頻率。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (選擇性) 若要確認您的組態記錄器已具備所需設定，請使用下列《describe-configuration-recorders》命令。

```
$ aws configservice describe-configuration-recorders
```

以下是回應範例。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

設 AWS Config 定為僅記錄您指定之資源類型的組態變更。如果您選擇停止記錄某個資源類型，則已記錄的組態項目會保持不變。

此指令會使用`--configuration-recorder`和`---recording-group`欄位。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> 錄音組和配置記錄器
> `--recording-group` 欄位指定記錄的資源類型。
> 此`--configuration-recorder`欄位會指定name組態錄製程式的預設錄製頻率，以及(`recordingMode`)。`roleArn`您也可以使用此欄位覆寫特定資源類型的記錄頻率。

1. 使用 `put-configuration-recorder` 命令，並在 `recordingGroup` 的 `resourceTypes` 欄位中傳遞一或多個資源類型，如下列範例所示。

   i. `recordingGroup.json` 檔案可指定 AWS Config 記錄的資源類型。

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

> **Note**
>
> 必要欄位和選用欄位

您必須先將 `allSupported` 和 `includeGlobalResourceTypes` 欄位設定為 `false` 或省略這些欄位，才能指定要包含在記錄中的資源類型。
當您在 `--recording-group` 的 `resourceTypes` 欄位中列出資源類型時，`recordingStrategy` 欄位為選用。

> **Note**
>
> 區域可用性
>
> 在指定 AWS Config 要追蹤的資源型態之前，請先勾選「依區域」的可用性「資源涵蓋範圍」，以查看您設定的「 AWS 區域」中是否支援資源型態 AWS Config。如果至少一個「區域」支援某個資源類型，則您可以 AWS Config 在所支援的所有「區域」中啟用該資源類型的記錄 AWS Config，即使您設定的「 AWS 區域」不支援指定的資源類型也一樣 AWS Config。

ii. `put-configuration-recorder` 會使用下列用於 `--configuration-recorder` 參數的欄位：

- `name`— 組態記錄程式的名稱。 AWS Config 建立組態記錄器時，會自動指定「default」的名稱。
- `roleARN`— 由組態記錄器承擔 AWS Config 並使用之 IAM 角色的 Amazon 資源名稱 (ARN)。
- `recordingMode`— 指定用來記錄組態變更的預設錄製頻率。 AWS Config AWS Config 支持連續錄製和每日錄製。連續記錄可讓您在發生變更時持續記錄組態變更。每日記錄可讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。
  - `recordingFrequency`— AWS Config 用來記錄組態變更的預設錄製頻率。

    > **Note**
    >
    > AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

  - `recordingModeOverrides` — 此欄位可讓您指定記錄模式的覆寫。其為 `recordingModeOverride` 物件的陣列。`recordingModeOverrides` 陣列中的每個 `recordingModeOverride` 物件都包含三個欄位：
    - `description` — 您為覆寫提供的描述。

- `recordingFrequency` — 會套用至覆寫中指定的所有資源類型的記錄頻率。
- `resourceTypes`— 逗號分隔清單，指定覆寫中 AWS Config 包含哪些資源類型。

> **Note**
>
> 必要欄位和選用欄位
>
> put-configuration-recorder 的 `recordingMode` 欄位為選用。依預設，組態記錄器的記錄頻率設定為連續記錄。

> **Note**
>
> 限制
>
> 下列資源類型不支援每日記錄：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> 對於記錄所有目前和未來支援的資源類型 (`ALL_SUPPORTED_RESOURCE_TYPES`) 記錄策略，這些資源類型會設定為「連續記錄」。

`configurationRecorder.json`檔案會指定`name`組態錄製程式的預設錄製頻率，以及 (`recordingMode`)。`roleArn`您也可以使用此欄位覆寫特定資源類型的記錄頻率。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
```

```
}
```

2. (選擇性) 若要確認您的組態記錄器已具備所需設定，請使用下列《describe-configuration-recorders》命令。

```
$ aws configservice describe-configuration-recorders
```

以下是回應範例。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
```

```
                ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

## 記錄頻率

AWS Config 支持連續錄製和每日錄製。連續記錄可讓您在發生變更時持續記錄組態變更。每日記錄可讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。

### 連續記錄

連續記錄的一些優點包括：

- 即時監控：連續記錄可立即偵測未經授權的變更或非預期的更改，進而增強您的安全性與合規性措施。
- 詳細分析：連續記錄可讓您對資源發生組態變更時進行深入分析，讓您能夠識別當下的模式和趨勢。

### 每日記錄

每日記錄的一些優點包括：

- 最小干擾：每日記錄可以為您提供更易於管理的資訊流，進而減少通知的頻率和警示疲勞。
- 成本效益：每日記錄可提供以較低頻率記錄資源變更的靈活性，進而降低與記錄的組態變更次數相關的成本。

> **Note**
>
> AWS Firewall Manager 取決於連續記錄來監視您的資源。如果您使用的是 Firewall Manager，建議您將記錄頻率設定為「持續」。

## 停止記錄資源

您可以隨時停 AWS Config 止記錄某種類型的資源。 AWS Config 停止記錄資源後，它會保留先前擷取的組態資訊，並且您可以繼續存取此資訊。

## 非記錄資源

如果未記錄資源，則只會 AWS Config 擷取該資源的建立和刪除，而不會擷取其他詳細資訊，而不會對您付出任何費用。建立或刪除未記錄的資源時，會 AWS Config 傳送通知，並在資源詳細資訊頁面上顯示事件。未記錄資源的詳細資訊頁面針對大多數的組態詳細資訊都僅會有 null 值，並且不會提供關係和組態變更的相關資訊。

> **Note**
>
> 如果資源已選取或先前已選取為要在組態記錄器中記錄的資源，則 `AWS::IAM::User`、`AWS::IAM::Policy`、 `AWS::IAM::Group`、`AWS::IAM::Role` 資源類型只會擷取建立 (`ResourceNotRecorded`) 和刪除 (`ResourceDeletedNotRecorded`) 狀態。

> **Note**
>
`ResourceNotRecorded`和`ResourceDeletedNotRecorded`不遵循資源類型的典型記錄時間的組態項目 (CI)。這些資源類型只會在組態記錄程式的週期性審核處理期間進行記錄，其頻率低於其他資源類型的頻率。

為已記錄資源 AWS Config 提供的關係資訊不受限制，因為缺少未記錄資源的資料。若記錄資源與未記錄資源有關，則該關係會在記錄資源的詳細資訊頁面上提供。

## AWS Config 規則和全域資源類型

2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的區域 AWS Config 中 AWS Config 記錄。這些全球 IAM 資源類型無法在 2022 年 2 月 AWS Config 之後支援的區域中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。

報告 2022 年 2 月前登錄的全球資源合規性的最佳做法

為避免不必要的評估，您應該只將具有這些全域資源範圍的 AWS Config 規則和一致性套件部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。這適用於 AWS Config 規則、組織 AWS Config 規則，以及由其他 AWS 服務建立的規則，例如 AWS Security Hub 和 AWS Control Tower。

如果未記錄在 2022 年 2 月之前上線的全域資源類型，建議您不要啟用下列定期規則，以避免不必要的評估：

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

在 2022 年 2 月之後上線的全球資源報告合規性的最佳做法

在 2022 年 2 月之後登入 AWS Config 錄製的全球資源類型，只會記錄在服務的主要區域中，以及分割區的 AWS GovCloud (美國西部)。 AWS GovCloud (US) 您應該將具有這些全域資源範圍的 AWS Config 規則和一致性套件部署到資源類型的本位目錄「地區」。如需詳細資訊，請參閱全域資源類型的本地區域。

# 記錄第三方資源的組態

記錄協力廠商資源或自訂資源類型的設定，例如內部部署伺服器、SAAS 監視工具和版本控制系統 (例如 GitHub)。您可以將協力廠商資源的組態資料發佈到中， AWS Config 並使用 AWS Config 主控台和

API 檢視和監視資源清查和組態歷程記錄。現在，您可以使用規則 AWS Config 來管理所有資源，並根據最佳實務來評估資源組態的合 AWS Config 規性。您也可以建立 AWS Config 規則或一致性套件，以根據最佳作法、內部政策和法規原則評估這些協力廠商資源。

> **Note**
>
> 如果您已配置 AWS Config 為記錄所有資源類型，則透過管理 (建立、更新或刪除) 的協力廠商資源 AWS CloudFormation 會自動追蹤 AWS Config 為組態項目。

先決條件：必須使用註冊協力廠商資源或自訂資源類型 AWS CloudFormation。

主題


- 步驟 1：設定您的開發環境
- 步驟 2：建立資源模型
- 步驟 3：產生成品
- 步驟 4：註冊您的資源
- 步驟 5：發佈資源組態
- 使用記錄和刪除協力廠商資源的組態狀態 AWS CLI
- 使用 API 管理第三方資源類型的組態狀態


## 步驟 1：設定您的開發環境

安裝和配置 AWS CloudFormation AWS CLI。 AWS CLI 可讓您建立自訂資源的模型和註冊。如需詳細資訊，請參閱自訂資源和什麼是 CloudFormation 指令行介面？ 。

## 步驟 2：建立資源模型

建立符合並驗證資源類型組態的資源提供者結構描述。

1. 使用 `init` 命令建立您的資源提供者專案，並產生所需的檔案。

   ```
   $ cfn init
   Initializing new project
   ```

2. `init` 命令會啟動精靈，引導您完成專案的設定，包括指定資源名稱。在此演練中，指定 `MyCustomNamespace::Testing::WordPress`。

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. 輸入資源的套件名稱。

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> 為了保證任何專案相依項都能正確解析，您可以使用 Maven 支援將產生的專案匯入 IDE。例如，如果您正在使用 IntelliJ IDEA，您將需要執行下列動作：
>
> - 從 檔案 選單內選擇 新建，再選擇 現存來源的專案。
> - 導覽至專案目錄
> - 在 匯入專案 對話方塊中，選擇 從外部模型匯入專案，再選擇 Maven。
> - 選擇 下一步 並接受任何預設值，以完成專案匯入。

4. 開啟包含資源結構描述的 `mycustomnamespace-testing-wordpress.json` 檔案。將下列結構描述複製並貼到 `mycustomnamespace-testing-wordpress.json` 中。

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
```

```
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. 驗證結構描述。

```
$ cfn validate
```

6. 更新資源提供者套件中自動產生的檔案，以檢視資源提供者結構描述更新。啟動資源提供者專案後， AWS CLI 會產生資源提供者的支援檔案和程式碼。重新產生程式碼以查看更新的結構描述。

```
$ cfn generate
```

> **Note**
>
> 使用 Maven 時，作為建置流程的一部分，`generate` 命令將在代碼編譯之前自動執行。因此，您的變更永遠不會與產生的程式碼同步。
>
> 請注意 CloudFormation CLI 必須位於 MAVEN/ 系統可以找到的位置。如需詳細資訊，請參閱《為開發延伸模組設定環境》。

如需完整流程的詳細資訊，請參閱《AWS CloudFormation中的模型資源提供者》。

## 步驟 3：產生成品

請執行下列命令來產生 `cfn submit` 的成品。

```
$ mvn package
```

## 步驟 4：註冊您的資源

AWS Config 不需要資源提供者處理程式來執行資源的組態追蹤。執行以下命令來註冊您的資源。

```
$ cfn submit
```

如需詳細資訊，請參閱註冊資源提供者以在 AWS CloudFormation 範本中使用。

## 步驟 5：發佈資源組態

確定:: 測試 MyCustomNamespace:: 的配置。WordPress

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

判斷來源的結構描述版本 ID AWS CloudFormation `DescribeType`。

在 AWS Config 看看這個資源配置是否被接受。若要評估符合性，您可以使用此資源撰寫 AWS Config 規則。如需詳細資訊，請參閱使用 AWS CLI 記錄和刪除協力廠商資源的組態狀態。

選用：若要自動記錄組態，請實作定期或以變更為基礎的組態收集器。

## 使用記錄和刪除協力廠商資源的組態狀態 AWS CLI

AWS CLI 這是一個統一的工具來管理您的 AWS 服務。只要下載和設定一個工具，您就可以從命令列控制多個 AWS 服務，並使用指令碼將它們自動化。若要取得有關 AWS CLI 和安裝 AWS CLI 工具的更多資訊，請參閱《AWS Command Line Interface 使用指南》中的以下內容。

- AWS Command Line Interface 使用者指南
- 設定 AWS Command Line Interface

如有必要，請輸入`aws configure`以配置 AWS CLI 以使用可用 AWS Config 彙總工具的「AWS 區域」。

主題

- 記錄組態項目

- 使用 AWS Config API 讀取組態項目
- 刪除第三方資源

## 記錄組態項目

使用下列程序，記錄第三方資源或自訂資源類型的組態項目：

請確定使用相符的結構描述來註冊資源類型 `MyCustomNamespace::Testing::WordPress`。

1. 開啟命令提示或終端機視窗。
2. 輸入以下命令：

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> 如類型結構描述中所定義，`writeOnlyProperties`會在記錄之前從組態中移除 AWS Config。這表示當透過讀取 API 取得組態時，這些值將不會出現。如需 `writeOnlyProperties` 的詳細資訊，請參閱《資源類型結構描述》。

## 使用 AWS Config API 讀取組態項目

1. 開啟命令提示或終端機視窗。
2. 輸入以下命令：

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. 按 Enter。

   您應該會看到類似下列的輸出：

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. 輸入以下命令：

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. 按 Enter。

   您應該會看到類似下列的輸出：

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

### 刪除第三方資源

您可以記錄要刪除之第三方資源或自訂資源類型的組態狀態。

- 輸入以下命令：

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

若成功的話，命令會在沒有其他輸出的情況下執行。

## 使用 API 管理第三方資源類型的組態狀態

您可以使用 PutResourceConfig 和 DeleteResource Config API 來管理協力廠商資源或自訂資源類型的組態狀態。如需詳細資訊，請參閱 API Reference (《 API 參考》)。

- PutResourceConfig
- DeleteResourceConfig

# 記錄受管執行個體的軟體組態

您可以使用 AWS Config 在 Amazon EC2 執行個體和現場部署伺服器上記錄軟體庫存變更。這可讓您查看軟體組態的歷史變更。例如，在受管理的 Windows 執行個體上安裝新的 Windows 更新時，會 AWS Config 記錄變更，然後將變更傳送至傳遞通道，以便您收到有關變更的通知。使用時 AWS Config，您可以查看代管執行個體安裝 Windows 更新的歷史記錄，以及它們在一段時間內的變更方式。

您必須完成下列步驟才能記錄軟體組態變更：

- 在 AWS Config中開啟受管執行個體清查資源類型的記錄。
- 將 EC2 和內部部署執行個體設定為 AWS Systems Manager中的受管執行個體。受管執行個體是指一種設定為搭配 Systems Manager 使用的機器。
- 使用 Systems Manager 庫存功能，從您的受管執行個體啟動軟體庫存收集。

> **Note**
>
> Systems Manager 現在支援為非受管執行個體建立組態項目

未受管執行個體的組態項目會有 `Key: “InstanceStatus”` 和 `Value: “Unmanaged”` 的補充組態。
未受管執行個體的組態項目不會收到其他更新
若要接收其他更新，組態項目必須是受管執行個體。

您也可以使用 AWS Config 規則來監視軟體組態變更，並收到變更是否符合規則或不相容的通知。舉例來說，如果您建立規則來檢查您的代管執行個體是否有指定的應用程式，而執行個體並未安裝該應用程式，則會將該執行個體 AWS Config 標記為不符合您的規則。如需受 AWS Config 管規則的清單，請參閱AWS Config 受管規則清單。

在 AWS Config中啟用軟體組態變更的記錄：

1. 在 AWS Config中開啟所有支援資源類型的記錄，或是選擇性記錄受管執行個體清查資源類型。如需詳細資訊，請參閱 錄製 AWS 資源。
2. 使用包含 AmazonSSM ManagedInstanceCore 受管政策的 Systems Manager 執行個體設定檔來啟動 Amazon EC2 執行個體。此 AWS 受管政策可讓執行個體使用 Systems Manager 服務的核心功能。

   如需您可以為 Systems Manager 新增執行個體設定檔的其他政策相關資訊，請參閱《AWS Systems Manager 使用者指南》中的建立 Systems Manager 的 IAM 執行個體設定檔。

   **Important**

   SSM 代理程式是為了在雲端中與 Systems Manager 通訊，而必須安裝在受管執行個體的 Amazon 軟體。如果是從 AMI 為下面其中一種作業系統建立 EC2 執行個體，則表示代理程式會預先安裝：

   - Windows Server 2003-2012 R2 AMI 發佈於 2016 月 11 月或之後。
   - Windows Server 2016 和 2019
   - Amazon Linux
   - Amazon Linux 2
   - Ubuntu Server 16.04
   - Ubuntu Server 18.04

   如果不是搭配預先安裝代理程式從 AMI 所建立的 EC2 執行個體，則您必須手動安裝代理程式。如需相關資訊，請參閱《AWS Systems Manager 使用者指南》中的下列主題：

- 在 Windows Server 的 EC2 執行個體上安裝和設定 SSM 代理程式
- 在 Linux 的 EC2 執行個體上安裝和設定 SSM 代理程式

3. 如《AWS Systems Manager 使用者指南》中的設定庫存收集所述，開始庫存收集。Linux 和 Windows 執行個體的程序都是相同的。

   AWS Config 可以記錄下列庫存類型的組態變更：

   - 應用程式 – 受管執行個體的應用程式清單，例如防毒軟體。
   - AWS 元件 — 代管執行個體的 AWS 元件清單，例如 AWS CLI 和 SDK。
   - 執行個體資訊 – 執行個體資訊，例如 OS 名稱和版本、網域，以及防火牆狀態。
   - 網路組態 – 組態資訊，例如 IP 地址、閘道和子網路遮罩。
   - Windows 更新 – 受管執行個體的 Windows 更新清單 (僅限 Windows 執行個體)。

   > **Note**
   > AWS Config 目前不支援記錄自訂庫存類型。

庫存收集是一種 Systems Manager 功能，而這類功能分組為操作管理、動作和變更、執行個體和節點，以及共用資源等類別。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的什麼是 Systems Manager？以及 Systems Manager 功能。

# 檢視 資源組態和歷史記錄

您可以檢視帳號中記錄的所有資源、指定期間內資源的組態變更，以及所選資源與所有相關資源的關係。 AWS Config 您也可以檢視時間表中 AWS Config 規則 顯示的評估資源的符合性狀態變更。

主題


- 查找發現的資源 AWS Config
- 檢視相容性資訊與評估結果
- 檢視組態和符合性歷程記

# 查找發現的資源 AWS Config

您可以使用 AWS Config 主控台 AWS CLI、和 AWS Config API 來查詢 AWS Config 已清查或發現的資源，包括目前未錄製的已 AWS Config 刪除資源和資源。 AWS Config 僅探索支援的資源類型。如需詳細資訊，請參閱 支援的資源類型。

## 查閱資源 (主控台)

您可以使用資源類型，或將資訊加上標籤以在 AWS Config 主控台中查閱資源。

查找資源（控制台）

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 資源庫存 頁面上，指定您要查閱之資源的搜尋選項：
   - 資源類別 — 選擇所有資源類別，或將結果縮小為僅限 AWS 資源。
   - 資源類型 – 選擇所有資源類型，或選取要篩選依據的資源。
   - 合規 – 選擇依任何合規狀態、合規性或不合規進行篩選。
3. AWS Config 列出符合搜尋選項的資源。您可以參閱下列資源資訊：
   - 資源識別符 – 資源識別符可能是資源 ID 或資源名稱 (若適用)。選擇資源識別符連結以檢視資源詳細資訊頁面。
   - 資源類型 – 列出的資源類型。
   - 符合性 — 根據規則 AWS Config 評估的資源狀態。

     如需詳細資訊，請參閱 檢視組態和符合性歷程記。

## 查閱資源 (AWS CLI)

您可以使用列 AWS CLI 出 AWS Config 已探索到的資源。

查閱資源 (AWS CLI)

使用 AWS Config service **`list-discovered-resources`** 命令：

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
```

```
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

若要檢視回應中所列資源的組態詳細資訊，請使用 `get-resource-config-history` 命令，並指定資源類型和 ID。如需此指令及其回應的範例 AWS Config，請參閱檢視組態歷史記錄。

### 查閱資源 (API)

您可以指定資源類型，並 AWS Config 傳回該類型資源的資源識別碼清單。如需詳細資訊，請參閱 AWS Config API 參考ResourceIdentifier中的。

若要查詢資源 (API) 的步驟

使用 ListDiscoveredResources 動作。

若要取得回應中列出之資源的組態詳細資訊，請使用GetResourceConfigHistory動作，然後指定資源類型和 ID。

## 檢視相容性資訊與評估結果

> **Important**
>
> 若要準確報告合規狀態，您必須記錄 `AWS::Config::ResourceCompliance` 資源類型。如需詳細資訊，請參閱重新編碼 AWS 資源。

您可以使用 AWS Config 主控台或 AWS SDK 來檢視規則和資源的符合性資訊和評估結果。

內容


- 檢視合規性 (主控台)
- 檢視合規性 (AWS SDK)

## 檢視合規性 (主控台)

若要檢視符合性 (主控台)

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 功能表中，確認區域選取器已設定為支援 AWS Config 規則的區域。如需受支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在導覽窗格中，選擇 Resources (資源)。在「資源庫存」頁面上，您可以依資源類別、資源類型和合規狀態進行篩選。如果適用，請選擇 納入已刪除的資源。下表顯示資源類型和適用於該資源之資源合規狀態的資源識別符。資源識別符可能是資源 ID 或資源名稱。
4. 從資源識別符資料行選取資源。
5. 選擇 資源時間軸 按鈕。您可以依組態事件、規範遵循事件或 CloudTrail 事件進行篩選。

> **Note**
>
> 或者，您可以直接在「資源庫存」頁面選擇資源名稱。若要從「資源詳細資訊」頁面存取資源時間軸，請選擇 資源時間軸 按鈕。

您也可以透過在 Resource inventory (資源清查) 頁面上查詢它們，來檢視您資源的合規。如需詳細資訊，請參閱 查找發現的資源 AWS Config。

## 檢視合規性 (AWS SDK)

取得規則的合 AWS Config 規資訊

下列程式碼範例會示範如何使用`DescribeComplianceByConfigRule`。

CLI

AWS CLI

取得 AWS Config 規則的合規性資訊

下列命令會針對一或多個資源違反的每個 AWS Config 規則傳回符合性 AWS 資訊：

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

在輸出中，每個CappedCount屬性的值表示有多少資源不符合相關規則。例如，下列輸出表示 3 個資源不符合名為的規則InstanceTypesAreT2micro。

輸出：

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeComplianceByConfigRule中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例擷取規則的相容性明細 ebs-optimized-instance，而規則沒有目前的評估結果，因此會傳回 UNADICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

輸出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

範例 2：此範例會傳回規則的不相容資源數目。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

輸出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeComplianceByConfigRule式參考中的。

取得資源的法規遵循 AWS 資訊

下列程式碼範例會示範如何使用`DescribeComplianceByResource`。

CLI

AWS CLI

取得資源的法規遵循 AWS 資訊

下列命令會針對 AWS Config 記錄且違反一或多個規則的每個 EC2 執行個體傳回合規資訊：

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

在輸出中，每個`CappedCount`屬性的值指示資源違反了多少規則。例如，下列輸出表示執行個體`i-1a2b3c4d`違反了 2 個規則。

輸出：

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeComplianceByResource中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例會檢查**AWS::SSM::ManagedInstanceInventory**資源類型是否符合「相容」相容性類型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

輸出：

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeComplianceByResource式參考中的。

取得規則的合 AWS Config 規摘要

下列程式碼範例會示範如何使用`GetComplianceSummaryByConfigRule`。

CLI

AWS CLI

取得 Con AWS fig 規則的合規摘要

下列命令會傳回符合規則的數目以及不相容的數目：

```
aws configservice get-compliance-summary-by-config-rule
```

在輸出中，每個`CappedCount`屬性的值表示有多少規則相容或不相容。

輸出：

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceSummaryByConfigRule中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會傳回不相容的 Config 規則數目。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

輸出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceSummaryByConfigRule式參考中的。

取得 AWS 資源的合規性摘要

下列程式碼範例會示範如何使用`GetComplianceSummaryByResourceType`。

CLI

AWS CLI

取得所有資源類型的符合性摘要

下列命令會傳回不相容的 AWS 資源數目以及相容的編號：

```
aws configservice get-compliance-summary-by-resource-type
```

在輸出中，每個`CappedCount`屬性的值表示有多少資源相容或不相容。

輸出：

```
{
    "ComplianceSummariesByResourceType": [
```

```
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

取得特定資源類型的符合性摘要

下列命令會傳回不相容的 EC2 執行個體數目以及符合規定的數目：

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

在輸出中，每個CappedCount屬性的值表示有多少資源相容或不相容。

輸出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
```

```
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceSummaryByResourceType中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會傳回相容或不相容的資源數量，並將輸出轉換為 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceSummaryByResourceType式參考中的。

若要取得 AWS Config 規則的評估結果

下列程式碼範例會示範如何使用`GetComplianceDetailsByConfigRule`。

CLI

AWS CLI

若要取得 Con AWS fig 規則的評估結果

下列命令會針對所有不符合名為的 AWS Config 規則的資源傳回評估結果`InstanceTypesAreT2micro`：

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

輸出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
```

```
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceDetailsByConfigRule中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例取得規則的評估結果， access-keys-rotated 並傳回依規定型態分組的輸出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

輸出：

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

範例 2：此範例會查詢「相容」資源之規則的符 access-keys-rotated 合性詳細資料。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

輸出：

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceDetailsByConfigRule式參考中的。

若要取得 AWS 資源的評估結果

下列程式碼範例會示範如何使用`GetComplianceDetailsByResource`。

CLI

AWS CLI

若要取得 AWS 資源的評估結果

下列命令會針對 EC2 執行個體`i-1a2b3c4d`不符合的每個規則傳回評估結果：

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

輸出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
```

```
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceDetailsByResource中的。

PowerShell

適用的工具 PowerShell

範例 1：指定資源的此範例迴避結果。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

輸出：

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceDetailsByResource式參考中的。

## 檢視組態和符合性歷程記

> **Important**
>
> 若要準確報告合規狀態，您必須記錄 `AWS::Config::ResourceCompliance` 資源類型。如需詳細資訊，請參閱重新編碼 AWS 資源。

您可以在 AWS Config 主控台中檢視對資源所做的組態、關係和變更數目。您可以使用檢視資源的組態歷史記錄 AWS CLI。

## 檢視組態詳細資訊 (主控台)

### 使用主控台檢視組態詳細資訊

當您在 資源庫存 頁面上查詢資源時，選擇資源識別符欄中的資源名稱或 ID 以檢視資源的詳細資訊頁面。詳細資訊頁面提供該資源的組態、關係以及對其所做的變更。

若要從資源詳細資訊頁面存取資源時間軸，請選擇 資源時間軸 按鈕。資源時間軸會為特定資源擷取 `ConfigurationItems` 在一段時間內的變更。您可以依組態事件、規範遵循事件或 CloudTrail事件進行篩選。

## 檢視組態詳細資訊 (AWS CLI)

### 使用檢視組態詳細資訊 AWS CLI

AWS Config 記錄的組態項目會視需求傳遞至指定的傳遞通道，做為組態快照集和組態串流。您可以使用檢 AWS CLI 視每個資源之組態項目的歷史記錄。

### 檢視組態歷史記錄

輸入 `get-resource-config-history` 命令，並指定資源類型和資源 ID，例如：

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
```

```
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```


如需回應欄位的詳細說明，請參閱Components of a Configuration Item和 支援的資源類型。

AWS Config中的 Amazon EBS 組態歷史記錄範例

AWS Config 會產生一組檔案，每個檔案都代表一個資源類型，並列出所記錄之該類型資源的所有組態變更。 AWS Config AWS Config 將此以資源為中心的組態歷史記錄匯出為啟用時指定的 Amazon S3 儲存貯體中的物件。 AWS Config每種資源類型的組態歷史記錄檔案都會包含自交付最後一個歷史記錄檔案之後，針對該類型的資源所偵測到的變更。通常每六小時會交付歷史記錄檔案一次。

以下是 Amazon S3 物件的內容範例，描述目前區域中所有 Amazon 彈性區塊存放區磁碟區的組態歷史記錄 AWS 帳戶。此帳戶中的磁碟區包含 `vol-ce676ccc` 和 `vol-cia007c`。自交付先前的歷史記錄檔案以來，磁碟區 `vol-ce676ccc` 有兩項組態變更，而磁碟區 `vol-cia007c` 有一項變更。

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
```

```
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
```

```
                "resourceType": "AWS::EC2::Instance",
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "vol-cia007c",
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
        "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
```

```
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
```

```
}
```

## 檢視資源的合規歷史記錄時間軸

AWS Config 支援根據評估儲存資源的合規性狀態變更 AWS Config 規則。資源合規歷史記錄會以時間軸的形式呈現。時間軸會為特定資源擷取 `ConfigurationItems` 在一段時間內的變更。如需的內容的資訊`ConfigurationItem`，請參閱 AWS Config API 參考ConfigurationItem中的。

您可以選擇使用或選擇退出在 AWS Config中記錄所有資源類型。如果您已選擇記錄所有資源類型，則會根據評估者 AWS Config AWS Config 規則自動開始記錄資源符合性歷程記錄。依預設，會 AWS Config 記錄所有支援資源的組態變更。您也可以僅選取特定的資源合規歷史記錄資源類型：`AWS::Config::ResourceCompliance`。如需詳細資訊，請參閱選取哪些資源 AWS Config 記錄。

### 使用資源檢視資源時間軸

從「資源庫存」頁面選擇特定資源來存取資源時間軸。

1. 從左側導覽選擇資源。
2. 在「資源庫存」頁面上，您可以依資源類別、資源類型和合規狀態進行篩選。如果適用，請選擇 納入已刪除的資源。

   下表顯示資源類型和適用於該資源之資源合規狀態的資源識別符。資源識別符可能是資源 ID 或資源名稱。
3. 從資源識別符資料行選取資源。
4. 選擇 資源時間軸 按鈕。您可以依組態事件、規範遵循事件或 CloudTrail 事件進行篩選。

> **Note**
>
> 或者，您可以直接在「資源庫存」頁面選擇資源名稱。若要從資源詳細資訊頁面存取資源時間軸，請選擇 資源時間軸 按鈕。

### 使用規則檢視資源時間軸

從「規則」頁面選擇特定規則來存取資源時間軸。

1. 從左側導覽選取規則。

2. 在「規則」頁面上，選擇評估相關資源的規則。如果畫面上沒有規則顯示，請使用新增規則按鈕新增規則。
3. 在「規則」詳細資訊頁面上，從「資源」評估表格中選取資源。
4. 選取 資源時間表 按鈕。資源時間軸會隨即顯示。

### 查詢合規歷史記錄

使 get-resource-config-history 用資源類型查詢資源符合性歷程記錄`AWS::Config::ResourceCompliance`。

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

您應該會看到類似下列的輸出：

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
    }
   ]
   "tags": {},
   "resourceType": "AWS::Config::ResourceCompliance",
   "resourceId": "AWS::S3::Bucket/configrules-bucket",
   "ConfigurationStateId": "1539799966921",
   "relatedEvents": [];
   "awsRegion": "us-west-2",
   "version": "1.3",
   "configurationItemMD5Hash": "",
   "supplementaryConfiguration": {},
   "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",
```

```
    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "AccountID"
   }
  ]
}
```

# 為您的 AWS Config 資源建立標籤

標籤是您指派給 AWS 資源的標籤。每個標籤皆包含由您定義的一個金鑰與一個選用值。標籤可讓您更輕鬆地管理、搜尋和篩選資源。

標籤可讓您以不同的方式分類您的 AWS 資源，例如依據目的、擁有者或環境。當您有許多相同類型的資源時，這將會很有用，因為您可以依據先前指派的標籤，快速識別特定的資源。您可以將一或多個標籤指派給您的AWS資源。每個標籤都有一個關聯值。

我們建議您為每種資源類型建立符合您需求的標籤金鑰。使用一致的標籤金鑰組可讓您更輕鬆的管理您的AWS資源。您可以根據您新增的標籤搜尋和篩選資源。

系統會嚴格將標籤解釋為字元字串，且不會自動指派至您的資源。您可以編輯標籤金鑰和值，並且可以隨時從資源移除標籤。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。若您將與現有標籤具有相同鍵的標籤新增到該資源，則新值會覆寫舊值。如果您刪除資源，也會刪除任何該資源的標籤。

您可以透過 AWS Command Line Interface (AWS CLI) 和 AWS Config API 參考來使用標籤。

## 標記相關的限制

以下列出適用於標籤的基本限制。

| 限制 | 描述 |
| --- | --- |
| 每個資源的標籤數上限 | 50 |
| 金鑰長度上限 | 128 個 UTF-8 編碼的 Unicode 字元 |
| 數值長度上限 | 256 個 UTF-8 編碼的 Unicode 字元 |
| 字首限制 | 標籤名稱或值不可使用 `aws:` 字首，因為它只保留給 AWS 使用。您不可編輯或刪除具此字首的 |

| 限制 | 描述 |
| --- | --- |
| | 標籤名稱或值。具此字首的標籤，不算在受資源限制的標籤計數內。 |
| 字元限制 | 標籤只能包含 Unicode 字母、數字、空格或這些符號：`_ . : / = + - @` |

## 以 AWS Config API 動作管理標籤

標籤型存取控制可用於以下三個資源：`ConfigurationAggregator`、`AggregationAuthorization` 和 `ConfigRule`。使用下列項目新增、更新、列出和刪除您資源的標籤。

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource`並`UntagResource`需要特定AWS Identity and Access Management (IAM) 許可來控制存取權。如需詳細資訊，請參閱《IAM 使用者指南》中的使用標籤金鑰控制存取權限。

# 使用 AWS Config 規則評估資源

用 AWS Config 於評估資 AWS 源的組態設定。您可以透過建立代表理想組態設定的 AWS Config 規則來執行此操作。 AWS Config 提供稱為受管規則的可自訂預先定義規則，以協助您開始使用。

AWS Config 規則的運作方式

當 AWS Config 持續追蹤您資源中發生的組態變更時，其也會檢查這些變更是否未遵循您規則中的任何條件。如果資源不符合規則，則會將資源和規則 AWS Config 標記為不相容。以下是 AWS Config 規則可能的評估結果：

- `COMPLIANT` - 規則通過合規檢查的條件。
- `NON_COMPLIANT` - 規則未通過合規檢查的條件。
- `ERROR` - 其中一個必要/選用參數無效、類型不正確，或格式不正確。
- `NOT_APPLICABLE` - 用於篩選出無法套用規則邏輯的資源。例如，alb-desync-mode-check 規則僅檢查 Application Load Balancer，並忽略 Network Load Balancer 和 Gateway Load Balancer。

例如，建立 EC2 磁碟區時， AWS Config 可以根據需要加密磁碟區的規則評估磁碟區。如果磁碟區未加密，則會將磁碟區和規則 AWS Config 標記為不相容。 AWS Config 還可以檢查您的所有資源，以了解整個帳戶的要求。例如， AWS Config 可以檢查帳戶中的 EC2 磁碟區數量是否保持在所需的總數內，或者帳戶是否用 AWS CloudTrail 於記錄。

服務連結規則

服務連結規則是一種獨特的受管規則類型，可支援其他 AWS 服務在您的帳戶中建立 AWS Config 規則。這些規則已預先定義為包含代表您呼叫其他 AWS 服務所需的所有權限。這些規則與 AWS 服務針對合規性驗證所建議 AWS 帳戶 的標準類似。如需詳細資訊，請參閱 服務連結規 AWS Config 則。

自訂規則

您也可以建立自訂規則，以評估尚 AWS Config 未記錄的其他資源。如需詳細資訊，請參閱 AWS Config 自訂規則 及 評估其他資源類型。

檢視符合性

主 AWS Config 控台會顯示規則和資源的合規性狀態。您可以查看 AWS 資源如何符合所需組態的整體規範，並瞭解哪些特定資源不合規。您也可以使用 AWS CLI、 AWS Config API 和 AWS SDK 向 AWS Config 服務提出要求以取得合規資訊。

透過使 AWS Config 用評估資源組態，您可以評估資源組態是否符合內部實務、產業準則和法規。

限制

如需每個帳戶及其他服務限制各區域的 AWS Config 規則數目上限，請參閱AWS Config 服務限制。

# 成本考量

如需與資源記錄相關聯的成本詳細資訊，請參閱AWS Config 定價。

建議：在刪除規則之前停止記錄資源符合性

強烈建議您在刪除帳戶中的規則之前停止記錄`AWS::Config::ResourceCompliance`資源類型。刪除規則會建立組態項目 (CI)，`AWS::Config::ResourceCompliance`且可能會影響您的 AWS Config 組態錄製程式成本。如果您要刪除評估大量資源類型的規則，這可能會導致記錄的 CI 數量激增。

最佳做法：

1. 停止錄製 `AWS::Config::ResourceCompliance`
2. 刪除規則
3. 開啟以下項目的錄製 `AWS::Config::ResourceCompliance`

建議：新增邏輯以處理自訂 lambda 規則的已刪除資源評估

建立 AWS Config 自訂 lambda 規則時，強烈建議您新增邏輯來處理已刪除資源的評估。

當評估結果標記為 `NOT_APPLICABLE` 時，其會被標記以進行刪除和清理。如果它們沒有標記為`NOT_APPLICABLE`，評估結果將保持不變，直到刪除規則為止，這可能會導致 CI 在刪除規則`AWS::Config::ResourceCompliance`時建立意外的尖峰。

如需如何設 AWS Config 定自訂 lambda 規則以傳回已刪除資源的相`NOT_APPLICABLE`關資訊，請參閱使用 AWS Config 自訂 lambda 規則管理已刪除的資源。

建議：提供自訂 lambda 規則範圍內的資源

AWS Config 如果規則的範圍不限於一或多個資源類型，則自訂 Lambda 規則可能會導致大量 Lambda 函數叫用。為了避免與您的帳戶相關聯的活動增加，強烈建議您為自訂 Lambda 規則提供範圍內的資源。如果未選取任何資源類型，則規則會針對帳戶中的所有資源叫用 Lambda 函數。

# 區域支援

目前，下列 AWS 區域支援「AWS Config 規則」功能。如需支援哪些區域的個別 AWS Config 規則清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com<br>config-fips.us-east-2.amazonaws.com | HTTPS<br>HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com<br>config-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com<br>config-fips.us-west-1.amazonaws.com | HTTPS<br>HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com<br>config-fips.us-west-2.amazonaws.com | HTTPS<br>HTTPS |
| 非洲 (開普敦) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| 亞太區域 (香港) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| 亞太區域 (海德拉巴) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| 亞太區域 (大阪) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 加拿大西部 (卡加利) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (米蘭) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (西班牙) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 歐洲 (蘇黎世) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| 以色列 (特拉維夫) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| 中東 (巴林) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| 中東 (阿拉伯聯合大公國) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

下列區域支援跨組 AWS 織中的成員帳戶部署 AWS Config 規則。

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 | |
|---|---|---|---|---|
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS | |

# AWS Config 規則的元件

AWS Config 規則會評估 AWS 資源的組態設定。規則有兩種類型：AWS Config 受管規則和 AWS Config 自訂規則。

AWS Config 受管規則是由建立的預先定義、可自訂的規則 AWS Config。如需受管規則的清單，請參閱AWS Config 受管規則清單。

AWS Config 自訂規則是您從頭開始建立的規則。建立 AWS Config 自訂規則的方法有兩種：使用 Lambda 函數 (AWS Lambda 開發人員指南)，以及使用 Guard (安全防護 GitHub儲存庫) (一種 policy-as-code 語言)。 AWS Config 使用建立的自訂規 AWS Lambda 則稱為AWS Config 自訂 Lambda 規則，而 AWS Config 使用安全警衛建立的自訂規則稱為AWS Config 自訂原則規則。

本頁討論 AWS Config 受管規則的中繼資料，以及如何使用規則開發套件 (RDK) 和規則開發套件程式庫 (RDKLib) 使用 Python 撰寫 AWS Config 自訂 AWS Config 規則的最佳作法。 AWS Config

如需瞭解如何建立 AWS Config 自訂原則規則的逐步解說，請參閱建立 AWS Config 自訂原則規則。如需瞭解如何建立 AWS Config 自訂 Lambda 規則的逐步解說，請參閱建立 AWS Config 自訂 Lambda 規則。

內容


- AWS Config 受管規則中繼資
- AWS Config 自訂規則結構
  - 撰寫規則
  - 規則邏輯


## AWS Config 受管規則中繼資

AWS Config 託管規則可以包含以下可變元數據：

defaultName

defaultName 是規則執行個體預設會取得的名稱。

description

規則描述提供規則評估的項目內容。 AWS Config 主控台有 256 個字元的限制。根據最佳實務，規則描述應該以 “Checks if” 開頭，並包含 NON_COMPLIANT 情境的描述。在規則說明中第一次提到時，服務名稱應以 AWS 或 Amazon 開頭完整寫入。例如， AWS CloudTrail 或 Amazon CloudWatch 代替 CloudTrail 或首 CloudWatch 次使用。後續參考則可以使用縮寫的服務名稱。

scope

scope 可決定作為規則目標的資源類型。如需支援的資源類型清單，請參閱支援的資源類型。

強制性InputParameter細節

「 compulsoryInputParameter詳細資訊」用於規則執行評估所需的參數。例如，`access-keys-rotated` 受管規則包含 `maxAccessKeyAge` 作為必要參數。如果參數為必要，則不會將其標記為 (選用)。每個參數都必須指定一個類型。類型可以是「字符串」，「整型」，「雙」，「CSV」，「布爾」和「StringMap」之一。

選擇性InputParameter詳細

「 optionalInputParameter詳細資訊」用於規則執行評估的選用參數。例如，`elasticsearch-logs-to-cloudwatch` 受管規則包含 `logTypes` 作為選用參數。每個參數都必須指定一個類型。類型可以是「字符串」，「整型」，「雙」，「CSV」，「布爾」和「StringMap」之一。

支援 EvaluationModes

supportedEvaluationModes 決定何時評估資源，無論是在部署資源之前或部署資源之後。

`DETECTIVE` 用於評估已部署的資源。這可讓您評估現有資源的組態設定。`PROACTIVE` 用於在部署資源之前對其進行評估。

這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是「非符合」(NON_COMPLUTION)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。 AWS

您可以指定 supportedEvaluationModes 至`DETECTIVEPROACTIVE`、或兩者`DETECTIVE`和`PROACTIVE`。您必須指定評估模式，且此欄位不能保持空白。

如需詳細資訊，請參閱《評估模式》。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。

> **Note**
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

## AWS Config 自訂規則結構

本節包含使用 AWS Config 規則開發套件 (RDK) 和 AWS Config 規則開發套件程式庫 (RDKLib) 的相關資訊。如需有關 RDK 或 RDKLib 的詳細資訊，請參閱和 aws-組態 aws-config-rdk rdklib 儲存庫。GitHub

### 撰寫規則

必要條件

1. 請依照《安裝 AWS CLI》中的步驟執行。
2. 請依照使用主控台設定或 AWS Config 使用設定中 AWS Config 的步驟進行 AWS CLI。如需支援地 AWS AWS Config 區的相關資訊，請從「區AWS 域服務」清單中選取您的地區。
3. 使用 pip 的建議方法來安裝 RDK：

```
pip install rdk
```

> **Note**
> 在使用 pip 之前，請確保其已安裝在您的機器上。

4. 使用 pip 的建議方法來安裝 RDKLib：

```
pip install rdklib
```

> **Note**
> 在使用 pip 之前，請確保其已安裝在您的機器上。

變更觸發規則

1. 若要建立由指定資源類型變更所觸發的規則，請執行下列命令：

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type
```

下列範例會建立由 AWS::IAM::User 資源類型變更所觸發的規則：

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
```

以下是您可以搭配 rdk create 命令用於變更觸發規則的旗標：

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

> **Note**
>
> 若要使用 RDKLib，必須將規則的執行期設定為 python3.6-lib。

執行 rdk create 之後，您應該會看到一個包含規則名稱和 3 個檔案的新目錄：

- *RULE_NAME*.py - 儲存規則邏輯的 Python 檔案
- *RULE_NAME*_test.py - 儲存規則單元測試的 Python 檔案
- parameters.json - 適用於 RDK 部署設定的 JSON 檔案

2. 下一步是撰寫規則邏輯。您只需要編輯 *RULE_NAME*.py 檔案。如果開啟 *RULE_NAME*.py 檔案，您就會看到一個可在其中新增規則邏輯的範本。以下是針對 MFA_ENABLED_RULE 產生的範本：

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
```

```
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

以下範例是含有規則邏輯之 MFA_ENABLED_RULE 範本的已編輯版本。此規則會檢查 IAM 使用者是否已啟用多重要素驗證 (MFA)。如果 IAM 使用者未啟用 MFA，則此規則為 NON_COMPLIANT。如需規則邏輯與範本中所提供方法的詳細資訊，請參閱規則邏輯。

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):

        username = configuration_item.get("resourceName")

        iam_client = client_factory.build_client("iam")

        response = iam_client.list_mfa_devices(UserName=username)

        # Scenario:1 IAM user has MFA enabled.
        if response["MFADevices"]:
            return [Evaluation(ComplianceType.COMPLIANT)]
```

```
        # Scenario:2 IAM user has MFA not enabled.
        annotation = "MFA needs to be enabled for user."
        return [Evaluation(ComplianceType.NON_COMPLIANT, annotation=annotation)]

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. 下一步是 AWS 使用控制台或安裝 RDKLib 層。 AWS AWS CLI RDKLib 的設計旨在作為 AWS Lambda 層運作。其允許您使用程式庫，而無需將程式庫納入部署套件中。

   - 若要使用 AWS 主控台安裝 RDKLib 層，請執行下列步驟：

     1. 開啟主 AWS Serverless Application Repository 控台，網址為 https://console.aws.amazon.com/serverlessrepo。
     2. 在左側導覽選單中，選擇 [可用的應用程式]。
     3. 搜尋`rdklib`並選擇 rdklib。
     4. 檢閱函數詳細資訊，然後予以部署。您不必進行任何變更。
     5. 在「概觀」頁面的「資源」區段中，複製 Lambda 層的 Amazon 資源名稱 (ARN)。部署規則時，您將需要 Lambda 層的 ARN。

   - 若要使用安裝 RDKLib 層 AWS CLI，請執行下列命令：

     1. 建立 RDKlib 層的變更集。

     ```
     aws serverlessrepo create-cloud-formation-change-set --application-id
      arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
     stack-name RDKlib-Layer
     ```

     其會傳回下列輸出：

     ```
     {
     ```

```
    "ApplicationId": "arn:aws:serverlessrepo:ap-
southeast-1:711761543063:applications/rdklib",
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
    "SemanticVersion": "0.1.0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
}
```

2. 執行變更集。您可以複製/貼上完整的變更集 ARN (ChangeSetId 從上一步中產生的輸出)，以自訂下列指令：

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. 傳回屬於已部署堆疊的所有相關聯資源。

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

其會傳回下列輸出：

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. 從上一個步驟產生的輸出中複製 Lambda 層的 ARN。Lambda 層的 ARN 是 `PhysicalResourceId`。

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. 下一步是提供 Lambda 函數所要擔任的角色。根據預設，Lambda 函數會嘗試擔任不允許使用的 AWSServiceRoleForConfig 角色。您必須使用 AWS_ConfigRole 受管政策建立角色。該角色必須與 AWS Config 具有信任關係，且 /rdk/ 路徑下的所有角色都應該擔任這個角色。信任政策範例如下：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

使用這個信任政策，執行下列命令：

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

現在，請執行下列命令以更新 ExecutionRoleName 的輸入參數，並提供角色名稱：

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-
name"}'
```

您也可以使用 `rdk modify` 透過下列旗標來更新變更觸發規則的詳細資訊：

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

5. 最後一個步驟是部署規則。若要部署規則，請從步驟 3 開始使用 Lambda 層的 ARN 執行下列命令：

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. 現在已部署規則。您可以使用主 AWS Config 控台來檢查規則是否如預期般運作。

定期規則

1. 若要建立針對指定資源類型定期觸發的規則，請執行下列命令：

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type --maximum-frequency EXECUTION_FREQUENCY
```

下列範例會建立針對 `AWS::IAM::User` 資源類型每 24 小時觸發一次的規則：

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
 --maximum-frequency TwentyFour_Hours
```

以下是您可以搭配 `rdk create` 命令用於定期規則的旗標：

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
```

```
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

> **Note**
>
> 若要使用 RDKLib，必須將規則的執行期設定為 `python3.6-lib`。

執行 `rdk create` 之後，您應該會看到一個包含規則名稱和 3 個檔案的新目錄：

- *RULE_NAME*`.py` - 儲存規則邏輯的 Python 檔案
- *RULE_NAME*`_test.py` - 儲存規則單元測試的 Python 檔案
- `parameters.json` - 適用於 RDK 部署設定的 JSON 檔案

2. 下一步是撰寫規則邏輯。您只需要編輯 *RULE_NAME*.py 檔案。如果開啟 *RULE_NAME*.py 檔案，您就會看到一個可在其中新增規則邏輯的範本。以下是針對 MFA_ENABLED_RULE 產生的範本：

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
```

```
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

此範本預設為變更觸發規則。反之，請將您的邏輯新增至 `evaluate_periodic` 方法中。以下範例是含有規則邏輯之 MFA_ENABLED_RULE 範本的已編輯版本。此規則會檢查 IAM 使用者是否已啟用多重要素驗證 (MFA)。如果 IAM 使用者未啟用 MFA，則此規則為 NON_COMPLIANT。如需規則邏輯與範本中所提供方法的詳細資訊，請參閱規則邏輯。

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):l

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        evaluations = []

        iam_client = client_factory.build_client("iam")

        paginator = iam_client.get_paginator("list_users")
        response_iterator = paginator.paginate()

        for response in response_iterator:
            for user in response["Users"]:
                username = user["UserName"]
                response = iam_client.list_mfa_devices(UserName=username)

                # Scenario:1 IAM user has MFA enabled.
                if response["MFADevices"]:
                    evaluations.append(Evaluation(ComplianceType.COMPLIANT,
 username, "AWS::IAM::User"))

                # Scenario:2 IAM user has MFA not enabled.
                if not response["MFADevices"]:
                    annotation = "MFA needs to be enabled for user."
                    evaluations.append(
                        Evaluation(ComplianceType.NON_COMPLIANT, username,
 "AWS::IAM::User", annotation=annotation)
                    )
```

```
        return evaluations

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. 下一步是 AWS 使用控制台或安裝 RDKLib 層。 AWS AWS CLI RDKLib 的設計旨在作為 AWS Lambda 層運作。其允許您使用程式庫，而無需將程式庫納入部署套件中。

   - 若要使用 AWS 主控台安裝 RDKLib 層，請執行下列步驟：

     1. 開啟主 AWS Serverless Application Repository 控台，網址為 https://console.aws.amazon.com/serverlessrepo。
     2. 在左側導覽選單中，選擇 [可用的應用程式]。
     3. 搜尋`rdklib`並選擇 rdklib。
     4. 檢閱函數詳細資訊，然後予以部署。您不必進行任何變更。
     5. 在「概觀」頁面的「資源」區段中，複製 Lambda 層的 Amazon 資源名稱 (ARN)。部署規則時，您將需要 Lambda 層的 ARN。

   - 若要使用安裝 RDKLib 層 AWS CLI，請執行下列命令：

     1. 建立 RDKlib 層的變更集。

     ```
     aws serverlessrepo create-cloud-formation-change-set --application-id
      arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
     stack-name RDKlib-Layer
     ```

     其會傳回下列輸出：

     ```
     {
         "ApplicationId": "arn:aws:serverlessrepo:ap-
     southeast-1:711761543063:applications/rdklib",
         "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
     a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
     ```

```
    "SemanticVersion": "0.1.0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
}
```

2. 執行變更集。您可以複製/貼上完整的變更集 ARN (ChangeSetId 從上一步中產生的輸出)，以自訂下列指令：

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. 傳回屬於已部署堆疊的所有相關聯資源。

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

其會傳回下列輸出：

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. 從上一個步驟產生的輸出中複製 Lambda 層的 ARN。Lambda 層的 ARN 是 `PhysicalResourceId`。

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. 下一步是提供 Lambda 函數所要擔任的角色。根據預設，Lambda 函數會嘗試擔任不允許使用的 `AWSServiceRoleForConfig` 角色。您必須使用 `AWS_ConfigRole` 受管政策建立角色。該角色必須與 AWS Config 具有信任關係，且 /rdk/ 路徑下的所有角色都應該擔任這個角色。信任政策範例如下：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

使用這個信任政策，執行下列命令：

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

現在，請執行下列命令以更新 `ExecutionRoleName` 的輸入參數，並提供角色名稱：

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-
name"}'
```

您也可以使用 `rdk modify` 透過下列旗標來更新定期規則的詳細資訊：

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

5. 最後一個步驟是部署規則。若要部署規則，請從步驟 3 開始使用 Lambda 層的 ARN 執行下列命令：

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. 現在已部署規則。您可以使用主 AWS Config 控台來檢查規則是否如預期般運作。

## 規則邏輯

下列 Python 程式碼範例是使用 RDK 和 RDKLib 撰寫規則的範本。您應該只在 `evaluate_parameters`、`evaluate_change` 和 `evaluate_periodic` 方法內進行變更，或者在需要時撰寫全新的函數以協助處理邏輯。如需使用 RDK 和 RDKlib 撰寫規則的先決條件，請參閱必要條件。

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ["AWS::Resource::Type"]

# When you create a rule, the class name will be the name you give the rule when you
 create it instead of ConfigRule
class ConfigRule (ConfigRule):

    def evaluate_parameters(self, rule_parameters):
        return rule_parameters

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ###############################
        # Add your custom logic here. #
        ###############################
```

```
    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        ################################
        # Add your custom logic here. #
        ################################

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = ConfigRule()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

APPLICABLE_RESOURCES

`APPLICABLE_RESOURCES` 是作為規則目標的資源類型。使用時，這應該是設定為規則目標資源類型的全域變數。如需支援的資源類型清單，請參閱支援的資源類型。

evaluate_parameters

Description

此方法用於檢查規則的輸入參數是否有效。最佳實務如下：

- 檢查列出的參數數目是否正確。
- 檢查參數名稱是否正確。
- 檢查參數值是否為正確的類型。
- 如果參數是整數，請檢查參數是否在合理的界限之間。
- 如果參數的可能選項數量有限，請檢查該參數是否為其中一個選項。
- 如果參數是字串，請檢查其長度是否合理，並修剪該值前後的任何空格。
- 檢查任何區分大小寫的處理是否適當。
- 盡可能限制參數輸入。例如，若您收到以逗號分隔的 ARN 清單，請確定僅允許使用逗號和 ARN 支援的字元。

參數

`rule_parameters` 是規則的輸入參數字典。

傳回語法

如果其中一個參數無效，則可能會引發 `InvalidParametersError` 錯誤：

```
from rdklib import InvalidParametersError
raise InvalidParametersError("Error message to display")
```

如果參數全都有效，該方法應傳回一個字典：

```
return valid_rule_parameters
```

evaluate_change

Description

此方法用於評估變更觸發規則的邏輯。

參數

`event`是由提供的 AWS Lambda 事件 AWS Config。這是一種 JSON 格式的文件，其中包含供 Lambda 函數處理的資料。如需範例，請參閱AWS Config 規則的範例事件。

`client_factory`是要用於規則的 ClientFactory 物件。該 ClientFactory 類創建或重複使用 boto3 客戶端，它為服務提供低級接口。 AWS boto3 客戶端方法與 AWS 服務 API 映射，這意味著服務操作映射到相同名稱的客戶端方法，並提供對相同操作參數的訪問。如需可用服務的清單，請參閱 Boto3 Docs 文件中的《可用服務》。

`client_factory` 的請求語法如下所示：

```
response = client_factory.build_client(
    service='string')
```

例如：

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> 需要 AWS 服務的 boto3 名稱。

`configuration_item` 是完整組態項目的字典，即使是大型組態項目也是如此。配置項目代表支持 AWS 資源的各種屬性的 point-in-time 視圖。如需的內容的資訊`ConfigurationItem`，請參閱 AWS Config API 參考ConfigurationItem中的。

`valid_rule_parameters` 是 `evaluate_parameters()` 方法的輸出。

傳回語法

該方法應傳回以下其中一或多項：

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> 報告已刪除資源的規則，應傳回 `NOT_APPLICABLE` 的評估結果，以避免不必要的規則評估。

您應該對所有不相容的評估使用註釋。例如：

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

evaluate_periodic

Description

此方法用於評估定期規則。

參數

`event`是由提供的 AWS Lambda 事件 AWS Config。這是一種 JSON 格式的文件，其中包含供 Lambda 函數處理的資料。如需範例，請參閱AWS Config 規則的範例事件。

`client_factory`是要用於規則的 ClientFactory 物件。該 ClientFactory 類創建或重複使用 boto3 客戶端，它為服務提供低級接口。 AWS boto3 客戶端方法與 AWS 服務 API 映射，這意味著服務操作映射到相同名稱的客戶端方法，並提供對相同操作參數的訪問。如需可用服務的清單，請參閱 Boto3 Docs 文件中的《可用服務》。

`client_factory` 的請求語法如下所示：

```
response = client_factory.build_client(
    service='string')
```

例如：

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> 需要 AWS 服務的 boto3 名稱。

`valid_rule_parameters` 是 `evaluate_parameters()` 方法的輸出。

傳回語法

該方法應傳回以下其中一或多項：

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> 報告已刪除資源的規則，應傳回 `NOT_APPLICABLE` 的評估結果，以避免不必要的規則評估。

您應該對所有不相容的評估使用註釋。例如：

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

## lambda_handler

Description

您不需要修改此方法。Lambda 處理常式用於處理事件。函數會在將`event`物件 AWS Lambda 傳遞給`handler`方法時執行。如需詳細資訊，請參閱 Python 中的 Lambda 函數處理常式。

參數

`event`是由提供的 AWS Lambda 事件 AWS Config。這是一種 JSON 格式的文件，其中包含供 Lambda 函數處理的資料。如需範例，請參閱AWS Config 規則的範例事件。

`context` 是 Lambda 在執行期傳遞給函數的物件。此物件提供的方法和屬性提供了函數在執行時可使用的資訊與方法。請注意，在較新版本的 Lambda 中已不再使用內容。

# AWS Config 規則的評估模式與觸發程式型態

將規則新增至帳號時，您可以指定何時在資源建立和管理程序中評估資源。 AWS Config 資源建立和管理程序稱為資源佈建。您可以選擇評估模式，以指定何時在此程序中評估資源。 AWS Config

根據規則， AWS Config 可以在部署資源之前、部署資源之後或兩者之後評估您的資源組態。在部署資源之前對其進行評估，即為主動評估。在部署資源之後對其進行評估，即為偵測評估。

您也可以選擇觸發類型，以指定 AWS Config 規則評估資源的頻率。當發生組態變更、定期排程或兩者同時發生時，即可評估資源。

## 觸發類型

將規則新增至帳戶後，請 AWS Config 將資源與規則條件進行比較。在此初始評估之後，每次觸發評估時都會 AWS Config 繼續執行評估。評估的觸發條件是和規則一起定義，並可包含下列類型：

| 觸發類型 | Description |
| --- | --- |
| 組態變更 | AWS Config 當有符合規則範圍的資源，且資源的組態發生變更時，會執行規則的評估。評估會在 AWS Config 傳送組態項目變更通知後執行。<br><br>您可以透過定義規則的範圍來選擇要進行評估的資源。範圍可包含下列項目：<br><br>• 一或多個資源類型<br>• 資源類型和資源 ID 的組合 |

| 觸發類型 | Description |
| --- | --- |
| | • 標籤鍵和值的組合<br>• 當任何記錄的資源建立、更新或刪除時<br><br>AWS Config 在偵測到符合規則範圍的資源變更時執行評估。您可以使用範圍來定義要進行評估的資源。 |
| 定期 | AWS Config 以您選擇的頻率執行規則的評估，例如，每 24 小時執行一次。 |
| 混合 | 部分規則同時具有組態變更和定期觸發條件。對於這些規則，請在偵測到組態變更時以及您指定的頻率 AWS Config 評估您的資源。 |

## 評估模式

評估模式共有兩種：

主動模式

使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是 AWS 「非符合」(NON_COMPLIGENTING)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。

資源類型結構描述會說明資源的屬性。您可以在 AWS CloudFormation 註冊表內的「AWS 公共擴展」中或使用以下 CLI 命令找到資源類型模式：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

如需詳細資訊，請參閱《 AWS CloudFormation 使用指南》中的 < 透過 AWS CloudFormation 登錄管理擴充功能 > 以及AWS 資源和屬性類型參考。

> **Note**
>
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

具有主動評估的受管規則清單

如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。

支援主動評估的資源類型清單

下列是支援主動評估的資源類型清單：

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

具有主動評估的範例規則

範例主動規則

1. 您可以將受 AWS Config 管規則新增至您的帳戶`S3_BUCKET_LOGGING_ENABLED`，以檢查 S3 儲存貯體是否已啟用記錄。
2. 對於評估模式，請選擇在 AWS 管理主控台中開啟**PROACTIVE**主動評估，或`EvaluationModes`在 PutConfigRuleAPI 中啟用。

開啟主動評估之後，您可以使用 StartResourceEvaluationAPI 和 GetResourceEvaluationSummaryAPI 來檢查帳戶中尚未部署到生產環境的值區是否未啟用記錄。這可讓您在部署之前測試資源組態，並重新評估是否要將資源部署到生產環境。

例如，從 StartResourceEvaluation API 開始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
```

```
                                        "ResourceType":"AWS::S3::Bucket",
                                        "ResourceConfiguration": "{\"BucketName\": \"my-
bucket\", \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您應該會在輸出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然後，使用`ResourceEvaluationId`與 GetResourceEvaluationSummary API 一起檢查評估結果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您應該會收到類似下列的輸出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration": "{\"BucketName\": \"my-bucket\",
 \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

    }
}
```

若要查看有關評估結果的其他資訊，例如哪些規則將資源標記為「非 _ 相容」，請使用 API。GetComplianceDetailsByResource

偵測模式

使用偵測評估來評估已部署的資源。這可讓您評估現有資源的組態設定。

偵測評估的範例規則

依變更而觸發的規則範例

1. 您將受管規則 (S3_BUCKET_LOGGING_ENABLED) 新增至您的帳戶，以檢查您的 S3 儲存貯體是否已啟用日誌記錄。
2. 規則的觸發類型為組態變更。 AWS Config 建立、變更或刪除 S3 儲存貯體時，執行規則的評估。
3. 當儲存貯體更新時，組態變更會啟動規則，而且 AWS Config 會評估儲存貯體是否符合規則。

定期規則範例

1. 您將受管規則 (IAM_PASSWORD_POLICY) 新增至您的帳戶。規則會檢查 IAM 使用者的密碼政策是否符合您的帳戶政策，例如要求最小長度或特定字元。
2. 規則的觸發類型是週期性的。 AWS Config 以您指定的頻率 (例如每 24 小時) 執行一次規則評估。
3. 每隔 24 小時就會啟動規則，並 AWS Config 評估 IAM 使用者的密碼是否符合規則。

同時具備組態變更及定期觸發的混合規則範例

1. 建立自訂規則，以評估帳戶中的 AWS CloudTrail 追蹤是否已開啟，以及是否針對所有區域進行記錄。
2. 您希 AWS Config 望在每次建立、更新或刪除追蹤時執行規則的評估。您也想 AWS Config 要每 12 小時執行一次規則。
3. 針對觸發條件類型，您可以為配置變更和定期觸發條件撰寫邏輯。如需詳細資訊，請參閱規AWS Config 則的元件：撰寫規則。

## 組態記錄器關閉時的規則評估

如果您關閉組態錄製程式，請 AWS Config 停止記錄資源組態的變更。這會透過下列方式影響您的規則評估：

- 定期規則會繼續依照指定的頻率執行評估。
- 受變更觸發的規則不會執行評估。

- 混合規則只會依照指定的頻率執行評估。規則不會針對組態變更執行評估。
- 若您執行具備組態變更觸發之規則的隨需評估，規則會評估資源最後一個已知狀態，即最後一個記錄的組態項目。

> **Important**
>
> 避免不必要的 AWS Config 評估
> 除非遭到刪除，否則定期規則和混合規則將繼續執行，即使您已關閉組態記錄器也是如此。這些規則只會評估在關閉組態記錄程式之前所記錄的組態項目，這表示這些規則會重現相同的評估結果，而不會有新資訊。關閉組態記錄器時，請刪除定期規則和混合規則，以避免不必要的活動和規則評估。

# AWS Config 受管規則

AWS Config 提供AWS 受管規則，這些規則是預先定義的可自訂規則， AWS Config 用來評估您的 AWS 資源是否符合一般最佳作法。例如，您可以使用受管規則快速開始評估您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是否加密，或特定標籤是否會套用到您的資源。主 AWS Config 控台會引導您完成設定和啟動受管規則的程序。您也可以使用 AWS Command Line Interface 或 AWS Config API 來傳遞定義受管規則組態的 JSON 程式碼。

您可以自訂受管規則的行為，以符合您的需求。例如，您可以定義規則的範圍，以限制要讓哪些資源 (EC2 執行個體或磁碟區等) 觸發規則的評估。您可以自訂規則的參數，以定義資源必須具備哪些屬性才能符合規則。例如，您可以自訂參數來指定安全群組應該封鎖特定連接埠號碼的傳入流量。

## 成本考量

如需與資源記錄相關聯的成本詳細資訊，請參閱AWS Config 定價。

建議：在刪除規則之前停止記錄資源符合性

強烈建議您在刪除帳戶中的規則之前停止記錄`AWS::Config::ResourceCompliance`資源類型。刪除規則會建立組態項目 (CI)，`AWS::Config::ResourceCompliance`且可能會影響您的 AWS Config 組態錄製程式成本。如果您要刪除評估大量資源類型的規則，這可能會導致記錄的 CI 數量激增。

最佳做法：

1. 停止錄製 `AWS::Config::ResourceCompliance`
2. 刪除規則
3. 開啟錄影功能 `AWS::Config::ResourceCompliance`

## 觸發類型

將規則新增至帳戶後，請 AWS Config 將資源與規則條件進行比較。在此初始評估之後，每次觸發評估時都會 AWS Config 繼續執行評估。評估觸發程序被定義為規則的一部分，它們可以包括下列類型。

| 觸發類型 | Description |
| --- | --- |
| 組態變更 | AWS Config 當有符合規則範圍的資源，且資源的組態發生變更時，會執行規則的評估。評估會在 AWS Config 傳送組態項目變更通知後執行。<br><br>您可以透過定義規則的範圍來選擇要進行評估的資源。範圍可包含下列項目：<br><br>• 一或多個資源類型<br>• 資源類型和資源 ID 的組合<br>• 標籤鍵和值的組合<br>• 當任何記錄的資源建立、更新或刪除時<br><br>AWS Config 當偵測到符合規則範圍的資源變更時，會執行評估。您可以使用範圍來定義要進行評估的資源。 |
| 定期 | AWS Config 以您選擇的頻率執行規則的評估，例如，每 24 小時執行一次。 |
| 混合 | 部分規則同時具有組態變更和定期觸發條件。對於這些規則，請在偵測到組態變更時以及您指定的頻率 AWS Config 評估您的資源。 |

# 評估模式

AWS Config 規則有兩種評估模式。

| 評估模式 | Description |
| --- | --- |
| 主動 | 使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是 AWS 「非符合」(NON_COMPLIGENTING)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。<br><br>如需詳細資訊，請參閱《評估模式》。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。 |
| 偵測 | 使用偵測評估來評估已部署的資源。這可讓您評估現有資源的組態設定。 |

> **Note**
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

主題


- AWS Config 受管規則清單
- 按評估模式排序的 AWS Config 受管理規則清單
- 按觸發類型排序的 AWS Config 受管理規則清單
- 按區域可用性分類的 AWS Config 受管規則清單
- 服務連結規 AWS Config 則
- 建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)


## AWS Config 受管規則清單

AWS Config 目前支援下列受管規則。

## 考量事項

受管規則的預設值

只有在使用 AWS 主控台時，才會預先填入針對受管理規則指定的預設值。不提供 API、CLI 或 SDK 的預設值。

不支援目錄儲存貯體

受管規則僅在評估 Amazon 簡單儲存服務 (Amazon S3) 資源時支援一般用途儲存貯體。 AWS Config 不會記錄目錄值區的組態變更。如需一般用途儲存貯體和目錄儲存貯體的詳細資訊，請參閱 Amazon S3 使用者指南中的儲存貯體概觀和目錄儲存貯體。

受管規則和全域 IAM 資源類型

2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。

為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

主題

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- EC2_IMDSV2_CHECK
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- 雲徑全讀 S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan

- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled

- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted

- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用安全防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-rds 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-服務器證書過期檢查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- Amazon CloudWatch Logs
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew

- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## access-keys-rotated

檢查作用中的 IAM 存取金鑰是否於 `maxAccessKeyAge` 指定的天數內進行輪換 (變更)。如果存取金鑰未在指定的期間內輪換，則表示規則為「NON_COMPLIANT」。預設值為 90 天。

> **Warning**
>
> 請勿將您的存取金鑰提供給未經授權的當事方，即便是協助尋找您的帳戶識別符也不妥。執行此作業，可能會讓他人能夠永久存取您的帳戶。安全最佳實務是在使用者不再需要密碼和存取金鑰時將其移除。

> **Note**
>
> 在主控台中標示為不相容的資源類型
>
> 如果此規則發現您的任何存取金鑰不相容，`AWS::IAM::User`資源類型也會在主控台中標示為不相容。 AWS
>
> 受管規則和全域 IAM 資源類型
>
> 2022 年 2 月之前登入的全球 IAM 資源類型
>
> (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
>
> 如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
>
> 為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。
>
> 限制
>
> 此規則不適用於 AWS 帳號根使用者存取金鑰。若要刪除或輪替您的 root 使用者存取金鑰，請使用您的 root 使用者認證登入 AWS Management Console 位置中的「我的安全認證」頁面https://aws.amazon.com/console/。

Identifier: (識別符：) ACCESS_KEYS_ROTATED

資源類型： AWS::IAM::User

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大AccessKey年齡, 類型：int, 預設：90

未進行輪換的天數上限。預設：90。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## account-part-of-organizations

檢查 AWS 帳戶是否為 Organ AWS izations 的一部分。如果帳號不是「 AWS 組織」的一部分，或「Organ AWS izations」主 AWS 帳號 ID 與規則參數不符，則該規則為「不符合」。`MasterAccountId`

> **Note**
>
> 受管規則和全域 IAM 資源類型
> 2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::Policy``AWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
> 如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
> 為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

識別符： ACCOUNT_PART_OF_ORGANIZATIONS

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

MasterAccountId (選擇性), 類型：字串

帳戶的主帳 AWS 戶 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## acm-certificate-expiration-check

檢查您帳戶中的 Certificate Manager 憑 AWS 證是否在指定天數內標示為過期。ACM 提供的憑證會自動更新。ACM 不會自動更新您匯入的憑證。如果您的憑證即將到期，則表示規則為「NON_COMPLIANT」。

識別符： ACM_CERTIFICATE_EXPIRATION_CHECK

資源類型： AWS::ACM::Certificate

觸發類型： Configuration changes (組態變更) 和 Periodic (定期)。

AWS 區域：所有支援的 AWS 地區

參數：

daysToExpiration (選擇性), 類型：int, 預設：14

指定規則將 ACM 憑證標記為未合規之前的天數。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## acm-certificate-rsa-check

檢查由「Certificate Manager」(ACM) 管理的 RSA 憑 AWS 證金鑰長度是否至少為 '2048' 位元。如果金鑰長度下限小於 2048 位元，則規則為「不相容」。

識別符：ACM_CERTIFICATE_RSA_CHECK

資源類型： AWS::ACM::Certificate

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## acm-pca-root-ca-disabled

檢查 AWS 私人憑證授權單位 (AWS 私有 CA) 是否具有已停用的根 CA。對於狀態為「DISABLED」的根 CA，則表示規則為「NON_COMPLIANT」。

識別符：ACM_PCA_ROOT_CA_DISABLED

資源類型： AWS::ACMPCA::CertificateAuthority

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

exemptedCAArns (選用), 類型：CSV

可啟用之 CA 的 Amazon Resource Name (ARN) 清單 (以逗號分隔)。此值可由其他 CA 提供，例如可啟用的特定根 CA 或中繼 CA。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## alb-desync-mode-check

檢查 Application Load Balancer (ALB) 是否已設定為使用者定義的去同步緩解模式。如果 ALB 去同步緩解模式與使用者定義的去同步緩解模式不相符，則表示規則為「NON_COMPLIANT」。

識別符：ALB_DESYNC_MODE_CHECK

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

desyncMode, 類型：CSV

以逗號分隔的清單，其中客戶可以選擇下列最多 2 個值：'defensive'、'strictest' 和 'monitor'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## alb-http-drop-invalid-header-enabled

檢查規則是否評估 AWS 應用程式負載平衡器 (ALB)，以確保它們設定為刪除 http 標頭。如果 routing.http.drop_invalid_header_fields.enabled 的值設定為 false，則表示規則為「NON_COMPLIANT」。

識別符：ALB_HTTP_DROP_INVALID_HEADER_ENABLED

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## alb-http-to-https-redirection-check

檢查是否在 Application Load Balancer 的所有 HTTP 接聽程式上設定 HTTP 到 HTTPS 重新導向。如果一或多個 Application Load Balancer 的 HTTP 接聽程式未設定 HTTP 到 HTTPS 重新導向，則表示規則為「NON_COMPLIANT」。如果其中一個 HTTP 接聽程式已轉送至 HTTP 接聽程式而非重新導向，則表示規則也是「NON_COMPLIANT」。

識別符： ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## alb-waf-enabled

檢查應用程式負載平衡器 (ALB) 上是否已啟用 AWS WAF。如果 key: waf 設定為 false，則表示規則為「NON_COMPLIANT」。

識別符：ALB_WAF_ENABLED

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

wafWebAclIds （可選），類型：CSV

檢查 ALB 關聯之 Web ACL ID (適用於 WAF) 或 Web ACL ARN (適用於 WAFV2) 的以逗號分隔清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gwv2-access-logs-enabled

檢查 Amazon API Gateway V2 階段是否已啟用存取日誌記錄。如果階段組態中沒有「存取 LogSettings」，則規則為「NON_ 相容」。

識別符：API_GWV2_ACCESS_LOGS_ENABLED

資源類型： AWS::ApiGatewayV2::Stage

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gwv2-authorization-type-configured

檢查 Amazon API Gatewayv2 API 路由是否設定了授權類型。如果授權類型為 NONE，則表示規則為「NON_COMPLIANT」。

識別符：API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

資源類型： AWS::ApiGatewayV2::Route

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

authorizationType (選用), 類型：字串

用於檢查 API 路由授權類型的參數。符合「自訂」、「 AWS_IAM」、「JWT」的字串參數有效。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gw-associated-with-waf

檢查 Amazon API Gateway API 階段是否正在使用 AWS WAF 網頁存取控制清單 (網頁 ACL)。如果未使用 AWS WAF Web ACL，或使用的 Web ACL 與規則參數中列出的內容不符，則該規則為「不符合」。 AWS

識別符：API_GW_ASSOCIATED_WITH_WAF

資源類型： AWS::ApiGateway::Stage

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

WebAclArns (選擇性), 類型：CSV

Web ACL Amazon Resource Name (ARN) 的清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gw-cache-enabled-and-encrypted

檢查 Amazon API Gateway 階段中的所有方法是否已啟用並加密快取。如果 Amazon API Gateway 階段中的任何方法未設定或加密快取，則表示規則為「NON_COMPLIANT」。

識別符： API_GW_CACHE_ENABLED_AND_ENCRYPTED

資源類型： AWS::ApiGateway::Stage

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gw-endpoint-type-check

檢查 Amazon API Gateway API 是否屬於規則參數 `endpointConfigurationType` 中指定的類型。如果 REST API 不符合規則參數中所設定的端點類型，則規則會傳回 NON_COMPLIANT。

識別符： API_GW_ENDPOINT_TYPE_CHECK

資源類型： AWS::ApiGateway::RestApi

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

端點 ConfigurationTypes, 類型：字串

以逗號分隔的允許 endpointConfigurationTypes清單。允許的值為 REGIONAL、PRIVATE 和 EDGE。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gw-execution-logging-enabled

檢查 Amazon API Gateway 階段中的所有方法是否已啟用日誌記錄。如果未啟用日誌記錄，或 `loggingLevel` 既不是 ERROR 也不是 INFO，則表示規則為「NON_COMPLIANT」。

識別符：API_GW_EXECUTION_LOGGING_ENABLED

資源類型: AWS::ApiGateway::Stage, AWS::ApiGatewayV2:: 階段

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

loggingLevel (選用), 類型：字串, 預設：ERROR,INFO

以逗號分隔的特定記錄層級清單 (例如，ERROR、INFO 或 ERROR,INFO)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gw-ssl-enabled

檢查 REST API 階段是否使用 SSL 憑證。如果 REST API 階段沒有相關聯的 SSL 憑證，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> `NOT_APPLICABLE`如果 GetIntegrationAPI `AWS` 以類型形式傳回，則會傳回此規則。

識別符：API_GW_SSL_ENABLED

資源類型： AWS::ApiGateway::Stage

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

CertificateIDs (選用), 類型：CSV

在 REST API 階段上設定之用戶端憑證 ID 的清單 (逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## api-gw-xray-enabled

檢查是否已在 Amazon API Gateway REST API 上啟用 AWS X-Ray 追蹤。如果啟用 X-Ray 追蹤，則表示規則為「COMPLIANT」，否則為「NON_COMPLIANT」。

識別符：API_GW_XRAY_ENABLED

資源類型： AWS::ApiGateway::Stage

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## approved-amis-by-id

檢查執行中的 EC2 執行個體是否使用指定的 Amazon Machine Image (AMI)。指定核准的 AMI ID 的清單。包含不在此清單上之 AMI 的執行中執行個體為「NON_COMPLIANT」。

識別符： APPROVED_AMIS_BY_ID

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

amiIds, 類型：CSV

AMI ID (以逗號分隔的清單，最多包含 21 個 AMI ID 或 1024 個字元，以先達到者為準)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## approved-amis-by-tag

檢查執行中的執行個體是否使用指定的 Amazon Machine Image (AMI)。指定識別 AMI 的標籤。包含沒有至少一個指定標籤之 AMI 的執行中執行個體為「NON_COMPLIANT」。

識別符： APPROVED_AMIS_BY_TAG

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

阿米斯價值 ByTag KeyAnd, 類型: StringMap, 預設：tag-key:tag-value,other-tag-key

按標籤分類的 AMI (最多 10 項的以逗號分隔的清單；例如 `tag-key:tag-value`，即 `tag-key1` 會將 AMI 與 `tag-key1` 進行比對，`tag-key2:value2` 比對具有 value2 的 `tag-key2`)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## appsync-associated-with-waf

檢查 AWS AppSync API 是否與 AWS WAFv2 網頁存取控制清單 (ACL) 相關聯。如果 AWS AppSync API 沒有與網頁 ACL 相關聯，則該規則為「不符合」規則。

識別符：APPSYNC_ASSOCIATED_WITH_WAF

資源類型:中 AWS::AppSync::Graph國

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

waf WebAcl ARN（可選），類型：CSV

授權 Web ACL 的 Amazon Resource Name (ARN) 清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## appsync-authorization-check

檢查 AWS AppSync API 是否使用允許的授權機制。如果正在使用未核准的授權機制，則表示規則為「NON_COMPLIANT」。

識別符：APPSYNC_AUTHORIZATION_CHECK

資源類型:中 AWS::AppSync::Graph國

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

AllowedAuthorization类型, 類型：CSV

以逗號分隔的允許 AWS AppSync 授權機制清單。允許的值為：'API_KEY'、'AWS_LAMBDA'、'AWS_IAM'、'OPENID_CONNECT'、'AMAZON_COGNITO_USER_P

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## appsync-cache-encryption-at-rest

檢查 AWS AppSync API 快取是否已啟用靜態加密。如果 " 為假，則此規則為「不符合 _ AtRestEncryptionEnabled」。

識別符：APPSYNC_CACHE_ENCRYPTION_AT_REST

資源類型:中 AWS::AppSync::Graph國

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## appsync-logging-enabled

檢查 AWS AppSync API 是否啟用了日誌記錄。如果未啟用日誌記錄，則該規則為「NON_COMPION」，或「字段LogLevel」既不是 ERROR 也不是全部。

識別符：APPSYNC_LOGGING_ENABLED

資源類型:中 AWS::AppSync::Graph國

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

fieldLoggingLevel (選擇性), 類型：CSV

以逗號分隔的特定欄位日誌記錄層級清單 (例如，ERROR、ALL)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

檢查 Amazon Athena 工作群組是否經過靜態加密。如果 Athena 工作群組未啟用靜態資料加密，則表示規則為「NON_COMPLIANT」。

識別符：ATHENA_WORKGROUP_ENCRYPTED_AT_REST

資源類型： AWS::Athena::WorkGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## aurora-last-backup-recovery-point-created

檢查是否已為 Amazon Aurora 資料庫叢集建立復原點。如果 Amazon Relational Database Service (Amazon RDS) DB 叢集沒有在指定時間範圍內建立對應的復原點，則該規則為「NON_COMPLIANT」。

識別符：AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型：AWS::RDS::DBCluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Aurora DB 叢集標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 Aurora DB 叢集 ID。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## aurora-meets-restore-time-target

確認 Amazon Aurora 資料庫叢集的還原時間是否符合指定的持續時間。如果 Aurora 資料庫叢集 LatestRestoreExecutionTimeMinutes 的時間大於 maxRestoreTime 分鐘，則該規則為「不相容」。

識別碼：AURORA_MEETS_RESTORE_TIME_TARGET

資源類型：AWS::RDS::DBCluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 Aurora DB 叢集標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則要檢查的 Aurora DB 叢集 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## aurora-mysql-backtracking-enabled

檢查 Amazon Aurora MySQL 叢集是否已啟用回溯功能。如果 Aurora 叢集使用 MySQL 且未啟用回溯功能，則表示規則為「NON_COMPLIANT」。

識別符：AURORA_MYSQL_BACKTRACKING_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域: 僅在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (倫敦)、亞太區域 (雪梨)、加拿大中歐 (寧夏) 地區

參數：

BacktrackWindowInHours (選擇性), 類型：double

要將 Aurora MySQL 叢集回溯的時間 (以小時為單位，最多 72 小時)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## aurora-resources-protected-by-backup-plan

檢查 Amazon Aurora 資料庫叢集是否受備份計畫的保護。如果 Amazon Relational Database Service (Amazon RDS) 資料庫叢集未受備份計畫保護，則該規則為「NON_COMPLIANT」。

識別符：AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型：AWS::RDS::DBCluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Aurora DB 叢集標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 Aurora DB 叢集 ID。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-capacity-rebalancing

檢查是否為使用多個執行個體類型的 Amazon EC2 Auto Scaling 群組啟用了容量重新平衡。如果未啟用容量重新平衡，則表示規則為「NON_COMPLIANT」。

識別符：AUTOSCALING_CAPACITY_REBALANCING

資源類型: AWS::AutoScaling::AutoScaling群組

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-group-elb-healthcheck-required

檢查與 Elastic Load Balancer 相關聯的 Amazon EC2 Auto Scaling 群組是否使用 Elastic Load Balancing 運作狀態檢查。如果 Amazon EC2 Auto Scaling 群組未使用 Elastic Load Balancing 運作狀態檢查，則表示規則為「NON_COMPLIANT」。

識別符： AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

資源類型: AWS::AutoScaling::AutoScaling群組

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。為了讓此規則在主動模式下傳回 COLUTION，StartResource評估 API 的資源組態結構描述必須包含下列輸入，編碼為字串：

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*有效值為 EC2 (預設值)、ELB 和 VPC_LATTICE。系統會保留 VPC_LATTICE 運作狀態檢查類型，以搭配 VPC Lattice 使用，此為預覽版本，可能會有所變更。如需詳細資訊，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的 Auto Scaling 執行個體的運作狀態檢查。

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-launchconfig-requires-imdsv2

檢查是否僅啟用 IMDSv2。如果啟動組態中未包含中繼資料版本，或者同時啟用中繼資料 V1 和 V2，則表示此規則為「NON_COMPLIANT」。

識別符：AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

資源類型： AWS::AutoScaling::LaunchConfiguration

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-launch-config-hop-limit

檢查中繼資料權杖可傳輸的網路跳轉數目。如果「中繼資料」回應躍點限制大於 1，則表示此規則為「NON_COMPLIANT」。

識別符：AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

資源類型： AWS::AutoScaling::LaunchConfiguration

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-launch-config-public-ip-disabled

檢查 Amazon EC2 Auto Scaling 群組是否透過啟動組態啟用公有 IP 地址。如果 Amazon EC2 Auto Scaling 群組的啟動組態已 AssociatePublicIpAddress 設定為「真」，則該規則為「不符合」規則。

識別符：AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

資源類型： AWS::AutoScaling::LaunchConfiguration

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-launch-template

檢查是否從 EC2 啟動範本建立了 Amazon Elastic Compute Cloud (EC2) Auto Scaling 群組。如果擴展群組不是從 EC2 啟動範本建立，則表示規則為「NON_COMPLIANT」。

識別符：AUTOSCALING_LAUNCH_TEMPLATE

資源類型: AWS::AutoScaling::AutoScaling群組

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-multiple-az

檢查 Auto Scaling 群組是否跨越多個可用區域。如果 Auto Scaling 群組未跨越多個可用區域，則表示規則為「NON_COMPLIANT」。

識別符： ：AUTOSCALING_MULTIPLE_AZ

資源類型: AWS::AutoScaling::AutoScaling群組

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

minAvailabilityZones (選擇性), 類型：int

預期可用區域的數量下限。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## autoscaling-multiple-instance-types

檢查 Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組是否使用多種執行個體類型。如果 Amazon EC2 Auto Scaling 群組只定義了一個執行個體類型，則表示此規則為「NON_COMPLIANT」。

識別符：AUTOSCALING_MULTIPLE_INSTANCE_TYPES

資源類型: AWS::AutoScaling::AutoScaling群組

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## backup-plan-min-frequency-and-min-retention-check

檢查備份計畫是否具有滿足所需頻率和保留期限的備份規則。如果復原點的建立頻率未達到指定頻率，或在指定期間之前到期，則表示規則為「NON_COMPLIANT」。

識別符：BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

資源類型： AWS::Backup::BackupPlan

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

requiredFrequencyValue (選擇性), 類型：int, 預設：1

所需備份頻率的數值。小時不可超過 24 個小時，天數不可超過 31 天。

requiredRetentionDays (選擇性), 類型：int, 預設：35

所需保留期 (以天為單位)。

requiredFrequencyUnit (選擇性), 類型：字串, 預設：天

所需備份頻率的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## backup-recovery-point-encrypted

檢查復原點是否已加密。如果復原點未加密，則表示規則為「NON_COMPLIANT」。

識別符：BACKUP_RECOVERY_POINT_ENCRYPTED

資源類型： AWS::Backup::RecoveryPoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## backup-recovery-point-manual-deletion-disabled

檢查備份保存庫是否具有連接的資源型政策，以防止刪除復原點。如果 Backup 儲存庫沒有以資源為基礎的策略或策略沒有適當的「拒絕」陳述式 (具備備份：DeleteRecovery點數、備份:和備份:權限的陳述式)，則該規則為「NON_COMPORT」。UpdateRecovery PointLifecycle PutBackupVaultAccessPolicy

識別符：BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

資源類型： AWS::Backup::BackupVault

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

principalArnList (選擇性), 類型：CSV

要檢查之規則的 AWS 身分和存取管理 (IAM) Amazon 資源名稱 (ARN) 清單 (逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## backup-recovery-point-minimum-retention-check

檢查復原點是否於指定期間之後過期。如果復原點的保留點小於所需的保留期間，則表示規則為「NON_COMPLIANT」。

識別符：BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

資源類型： AWS::Backup::RecoveryPoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

requiredRetentionDays (選擇性), 類型：int, 預設：35

所需保留期 (以天為單位)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## beanstalk-enhanced-health-reporting-enabled

檢查 E AWS lastic Beanstalk 環境是否設定為增強健全狀況報告。如果已為環境設定增強型運作狀態報告，則表示規則為「COMPLIANT」。如果已為環境設定基本運作狀態報告，則表示規則為「NON_COMPLIANT」。

識別符：BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

資源類型： AWS::ElasticBeanstalk::Environment

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## clb-desync-mode-check

檢查 Classic Load Balancer (CLB) 是否設定了使用者定義的去同步緩解模式。如果 CLB 去同步緩解模式與使用者定義的去同步緩解模式不相符，則表示規則為「NON_COMPLIANT」。

識別符：CLB_DESYNC_MODE_CHECK

資源類型： AWS::ElasticLoadBalancing::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

desyncMode, 類型：CSV

以逗號分隔的值清單。您最多可以選擇兩項。有效值包括 'Defensive'、'Strictest' 和 'Monitor'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## clb-multiple-az

檢查 Classic Load Balancer 是否跨越數個可用區域 (AZ)。如果 Classic Load Balancer 跨越少於 2 個 AZ，或者未跨越 `minAvailabilityZones` 參數中提到的 AZ 數目 (若有提供)，則表示規則為「NON_COMPLIANT」。

識別符： CLB_MULTIPLE_AZ

資源類型： AWS::ElasticLoadBalancing::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

minAvailabilityZones (選擇性), 類型：int

預期之 AZ 的所需最小數量。有效值介於 2 到 10 之間。如未指定參數，則預設值為 2。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudformation-stack-drift-detection-check

檢查 AWS CloudFormation （AWS CloudFormation）堆棧的實際配置是否與預期的配置不同或已漂移。如果堆疊的一個或多個資源與所預期的組態不同，堆疊就視為已偏離。當堆疊偏離狀態為 IN_SYNC，則規則和堆疊為 COMPLIANT。當堆疊偏離狀態為「已漂移」，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則會在您帳戶中的每個堆疊上執行 DetectStackDrift 作業。此 DetectStackDrift 作業最多可能需要幾分鐘的時間，具體取決於堆疊中包含的資源數目。鑑於此規則的最長執行時間限制為 15 分鐘，因此規則可能會在完成帳戶中所有堆疊的評估之前逾時。
> 如果您遇到此問題，建議您使用標籤來限制規則範圍內的堆疊數目。您可以執行下列作業：
>
> 1. 將堆疊分成群組，每個堆疊都有不同的標籤。
> 2. 將相同的標籤套用至該群組中的所有堆疊。
> 3. 在您的帳戶中有多個此規則的執行個體，每個執行個體都有不同的標籤範圍。這允許規則的每個執行個體僅處理擁有在其範圍中提到之對應標籤的堆疊。

Identifier: (識別符：) CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

資源類型： AWS::CloudFormation::Stack

觸發類型： Configuration changes (組態變更) 和 Periodic (定期)。

AWS 區域：所有支援的 AWS 地區

參數：

雲形 RoleArn, 類型：字串

具有政策許可的 IAM 角色的 Amazon 資源名稱 (ARN)，可偵測 AWS CloudFormation 堆疊的漂移。如需角色所需 IAM 許可的詳細資訊，請參閱偵測堆疊和資源的非受管組態變更 |《 AWS CloudFormation 使用者指南》中的偵測偏移時的考量事項。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudformation-stack-notification-check

檢查 CloudFormation 堆疊是否會將事件通知傳送至 Amazon SNS 主題。選擇性檢查是否使用指定的 Amazon SNS 主題。如果 CloudFormation 堆疊不傳送通知，則該規則為「不符合 _ 規範」。

識別符： CLOUDFORMATION_STACK_NOTIFICATION_CHECK

資源類型： AWS::CloudFormation::Stack

觸發類型： Configuration changes (組態變更)

AWS 區域: 僅適用於中國 (北京)、亞太區域 (孟買)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (中國雪梨)、加拿大 (寧格) 夏) 地區

參數：

snsTopic1 (選用), 類型：字串

SNS 主題 ARN。

snsTopic2 (選用), 類型：字串

SNS 主題 ARN。

snsTopic3 (選用), 類型：字串

SNS 主題 ARN。

snsTopic4 (選用), 類型：字串

SNS 主題 ARN。

snsTopic5 (選用), 類型：字串

SNS 主題 ARN。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-accesslogs-enabled

檢查 Amazon CloudFront 分發是否設定為將存取日誌交付到 Amazon S3 儲存貯體。如果 CloudFront 發行版沒有設定記錄，則規則為「NON_COLUTION」。

識別符：CLOUDFRONT_ACCESSLOGS_ENABLED

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

S3 BucketName (選擇性), 類型：字串

存放伺服器存取日誌的 Amazon S3 儲存貯體名稱。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-associated-with-waf

檢查 Amazon CloudFront 分發是否與 Web 應用程式防火牆 (WAF) 或 WAFv2 網頁存取控制清單 (ACL) 相關聯。如果 CloudFront 分配未與 WAF 網頁 ACL 相關聯，則該規則為「不符合」規則。

識別符：CLOUDFRONT_ASSOCIATED_WITH_WAF

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

wafWebAclIds （可選），類型：CSV

以逗號分隔的 WAF web ACL ID 或 WAFV2 web ACL Amazon Resource Name (ARN) 清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-custom-ssl-certificate

檢查與 Amazon CloudFront 分發關聯的憑證是否為預設 SSL 憑證。如果 CloudFront 發行版使用預設 SSL 憑證，則該規則為「NON_ 相容」。

識別符：CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-default-root-object-configured

檢查 Amazon CloudFront 分發是否設定為傳回預設根物件的特定物件。如果 Amazon CloudFront 分發沒有設定預設根物件，則該規則為「不符合 NON_ 規範」。

識別符：CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-no-deprecated-ssl-protocols

檢查 CloudFront 發行版是否使用已淘汰的 SSL 通訊協定在 CloudFront 邊緣位置和自訂來源之間進行 HTTPS 通訊。如果有任何「通訊OriginSsl協定」包含「SSLv3」，則此規則對於 CloudFront 散佈而言是「不符合 _」的規則。

識別符：CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-origin-access-identity-enabled

檢查使用 Amazon S3 來源類型的 CloudFront 分發是否已設定原始存取身分。如果 CloudFront 分發由 S3 支援，且任何來源類型未設定 OAI，或者來源不是 S3 儲存貯體，則該規則為 NON_COMPODE。

> **Note**
>
> 如果來源不是 S3 儲存貯體，則規則不會傳回「NOT_APPLICABLE」。

識別符：CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-origin-failover-enabled

檢查原始群組是否已設定為 Amazon 原始群組中至少兩個來源的分佈 CloudFront。如果沒有用於分佈的原始群組，則表示規則為「NON_COMPLIANT」。

識別符：CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-s3-origin-access-control-enabled

檢查具有 Amazon 簡單儲存服務 (Amazon S3) 原始類型的 Amazon CloudFront 分發是否已啟用來源存取控制 (OAC)。對於沒有啟用 OAC 的 Amazon S3 來源的 CloudFront 散發，此規則是「不符合 _ 規範」的規則。

識別符：CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-s3-origin-non-existent-bucket

檢查 Amazon CloudFront 發行版是否指向不存在的 S3 儲存貯體。如果 CloudFront 發佈點指向不存在的 S3 儲存貯體，則該規則為 OriginConfig「不符合 _」。該規則不會評估具有靜態網站託管的 S3 儲存貯體。

識別符：CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

資源類型： AWS::CloudFront::Distribution

觸發類型：定期

AWS 區域：只有在中國 (北京)、美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-security-policy-check

檢查 Amazon CloudFront 分發是否使用 TLSv1.2 或更高版本的最低安全政策和 TLSv1.2 或更高版本的密碼套件進行檢視器連線。如果發行版本低於 TLSv1.2_2018，則此規則對於 CloudFront 發佈而言 minimumProtocolVersion 是「不符合 _」的規則。

識別符：CLOUDFRONT_SECURITY_POLICY_CHECK

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## EC2_IMDSV2_CHECK

檢查 Amazon CloudFront 分發是否使用自訂 SSL 憑證，並設定為使用 SNI 來提供 HTTPS 請求。如果已與自訂 SSL 憑證相關聯，但 SSL 的支援方法為專用 IP 地址，則表示規則為「NON_COMPLIANT」。

識別符：CLOUDFRONT_SNI_ENABLED

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-traffic-to-origin-encrypted

檢查 Amazon CloudFront 分發是否正在加密到自訂來源的流量。如果「OriginProtocol政策」為「僅限 HTTP」或「政策」是「匹配查看器」且「OriginProtocol策略」為「全部」，則該規則為「不符合_」。ViewerProtocol

識別符：CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudfront-viewer-policy-https

檢查您的 Amazon CloudFront 分發是否使用 HTTPS (直接或透過重新導向)。如果將或的 ViewerProtocolPolicy 值設定為「允許全部」，則規則為「不相容」。 DefaultCacheBehavior CacheBehaviors

識別符： CLOUDFRONT_VIEWER_POLICY_HTTPS

資源類型： AWS::CloudFront::Distribution

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 雲徑全讀 S3-數據事件檢查

檢查是否已啟用 AWS CloudTrail 多區域追蹤，並記錄儲存貯體的所有讀取 S3 資料事件。如果沒有多區域追蹤記錄全部讀取所有目前和 future S3 儲存貯體的 S3 資料事件類型，則該規則為 NON_COMPLUTION。

識別碼：雲路 _ 全部 _ 讀取 _ S3_ 資料 _ 事件 _ 檢查

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 雲跟踪全寫 S3 數據事件檢查

檢查是否已啟用 AWS CloudTrail 多區域追蹤，並記錄儲存貯體的所有寫入 S3 資料事件。如果沒有多區域追蹤記錄全部寫入所有目前和 future S3 儲存貯體的 S3 資料事件類型，則該規則為 NON_COMPLUTION。

識別碼：雲通路 _ 全部 _ 寫入 _ S3_ 資料 _ 事件 _ 檢查

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 雲通道 S3-桶訪問日誌

檢查 AWS CloudTrail 日誌的 S3 儲存貯體組態是否已啟用 Amazon S3 伺服器存取記錄。如果 CloudTrail 追蹤至少有一個 S3 儲存貯體未啟用 S3 伺服器存取記錄，則該規則為「NON_COMPODE」。

識別碼：雲通道 _ S3_ 儲存區 _ 存取記錄

資源類型： AWS::CloudTrail::Trail

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 雲路-s3 桶公共訪問禁止

檢查 AWS CloudTrail 日誌的 S3 儲存貯體組態是否封鎖公開存取。如果 CloudTrail 追蹤的至少有一個 S3 儲存貯體可公開存取，則該規則為「NON_COMPON_」。

標識符：雲通道 _S3_ 桶 _ 公共訪問 _ 禁止

資源類型： AWS::CloudTrail::Trail

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudtrail-s3-dataevents-enabled

檢查是否至少有一個 AWS CloudTrail 追蹤正在記錄所有 S3 儲存貯體的 Amazon 簡單儲存服務 (Amazon S3) 資料事件。如果有追蹤或沒有追蹤記錄 S3 資料事件，則表示規則為「NON_COMPLIANT」。

識別符： CLOUDTRAIL_S3_DATAEVENTS_ENABLED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

S3 BucketNames (選擇性), 類型：字串

> 應啟用資料事件日誌記錄的 S3 儲存貯體名稱清單 (以逗號分隔)。所有 S3 儲存貯體的預設行為檢查。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudtrail-security-trail-enabled

檢查至少有一個以安全性最佳做法定義的 AWS CloudTrail 追蹤。如果至少有一個追蹤符合下列所有條件，則表示規則為「COMPLIANT」：

- 記錄全域服務事件
- 是一個多區域追蹤
- 已啟用日誌檔驗證
- 透過 KMS 金鑰進行加密
- 記錄讀取和寫入的事件
- 記錄管理事件
- 不排除任何管理事件

如果沒有追蹤符合上述所有準則，則表示規則為「NON_COMPLIANT」。

識別符：CLOUDTRAIL_SECURITY_TRAIL_ENABLED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudwatch-alarm-action-check

檢查 CloudWatch 警示是否已針對「警示」、「不足資料」或「確定」狀態設定動作。選擇性地檢查是否有任何動作符合具名 ARN。如果沒有針對警示或選用參數指定任何動作，則表示規則為「NON_COMPLIANT」。

識別符： CLOUDWATCH_ALARM_ACTION_CHECK

資源類型： AWS::CloudWatch::Alarm

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

警報 ActionRequired, 類型：字串, 預設：true

警示有至少一個動作。

DataAction需要不足, 類型：字串, 預設：true

警示會在警示從任何其他狀態轉移為 INSUFFICIENT_DATA 狀態時有至少一個動作。

好 ActionRequired, 類型：字串, 預設：false

警示會在警示從任何其他狀態轉移為 OK 狀態時有至少一個動作。

action1 (選用), 類型：字串

要執行的動作，指定為 ARN。

action2 (選用), 類型：字串

要執行的動作，指定為 ARN。

action3 (選用), 類型：字串

要執行的動作，指定為 ARN。

action4 (選用), 類型：字串

要執行的動作，指定為 ARN。

action5 (選用), 類型：字串

要執行的動作，指定為 ARN。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudwatch-alarm-action-enabled-check

檢查 Amazon CloudWatch 警示動作是否處於啟用狀態。如果 CloudWatch 警示動作未處於啟用狀態，則規則為「NON_COLUTION」。

識別符：CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

資源類型： AWS::CloudWatch::Alarm

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudwatch-alarm-resource-check

檢查資源類型是否具有指定指標的 CloudWatch 警示。針對資源類型，您可指定 EBS 磁碟區、EC2 執行個體、Amazon RDS 叢集或 S3 儲存貯體。如果指定的量度具有資源 ID 和 CloudWatch 警示，則規則為「相容」。

識別符：CLOUDWATCH_ALARM_RESOURCE_CHECK

資源類型: AWS::EC2::Instance AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceType, 類型：字串

AWS 資源類型。該值可以是下列其中一項： AWS::EC2::Volume、 AWS::EC2::Instance、AWS::RDS::DBCluster, or AWS::S3::Bucket。

metricName, 類型：字串

與警示相關聯之指標的名稱 (例如，EC2 執行個體的 'CPUUtilization')。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudwatch-alarm-settings-check

檢查具有指定測量結果名稱的 CloudWatch 警示是否具有指定的設定值。

識別符： CLOUDWATCH_ALARM_SETTINGS_CHECK

資源類型： AWS::CloudWatch::Alarm

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

metricName, 類型：字串

與警示關聯的指標名稱。

threshold (選用), 類型：int

比較指定統計資料的值。

evaluationPeriods (選用), 類型：int

執行資料和指定閾值比較作業的週期。

period (選用), 類型：int, 預設：300

將套用指定統計資料的期間 (秒)。

comparisonOperator (選用), 類型：字串

用於比較指定統計值和臨界值的作業 (例如，'GreaterThan臨界值')。

statistic (選用), 類型：字串

與警示關聯之指標的統計資料 (例如，'Average' 或 'Sum')。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudwatch-log-group-encrypted

檢查 Amazon CloudWatch 日誌群組是否使用任何 AWS KMS 金鑰或指定的 AWS KMS 金鑰識別碼加密。如果 CloudWatch 記錄群組未使用 KMS 金鑰加密，或使用規則參數中未提供的 KMS 金鑰加密，則該規則為 NON_COMPOFILE。

識別符： CLOUDWATCH_LOG_GROUP_ENCRYPTED

資源類型： AWS::Logs::LogGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

KmsKeyId (選擇性), 類型：字串

用來加密日誌群組之 KMS 金鑰的 ID Amazon Resource Name (ARN)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloud-trail-cloud-watch-logs-enabled

檢查 AWS CloudTrail 追蹤是否設定為將記錄檔傳送至 CloudWatch 記錄檔。如果系統線的 CloudWatchLogsLogGroupArn 屬性為空，則系統線為「非 _ 相容」。

Identifier: (識別符：) CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

資源類型： AWS::CloudTrail::Trail

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

預期DeliveryWindowAge （可選），類型：int

最近傳遞至符合規範之 CloudWatch 記錄檔的保留天數上限 (以小時為單位)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloudtrail-enabled

> **Important**
>
> 針對此規則，規則識別符 (CLOUD_TRAIL_ENABLED) 和規則名稱 (cloudtrail-enabled) 不同。

檢查您的 AWS 帳戶中是否已啟用 AWS CloudTrail 追蹤。如果未啟用追蹤，則表示規則為「NON_COMPLIANT」。此規則可選擇性地檢查特定 S3 儲存貯體、Amazon Simple Notification Service (Amazon SNS) 主題和 CloudWatch 日誌群組。

識別符： CLOUD_TRAIL_ENABLED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

s3 BucketName (選擇性的), 類型：字串

CloudTrail 要傳遞日誌檔的 S3 儲存貯體名稱。

snsTopicArn (選擇性), 類型：字串

用於通知的 CloudTrail SNS 主題 ARN。

雲端 WatchLogsLogGroupArn (選擇性), 類型：字串

CloudWatch 要將資料傳送 CloudTrail 至的記錄群組 ARN。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloud-trail-encryption-enabled

檢查 AWS CloudTrail 是否設定為使用伺服器端加密 (SSE) AWS Key Management Service (AWS KMS) 加密。如果已定義，則規則 KmsKeyId 為「相容」。

識別符： CLOUD_TRAIL_ENCRYPTION_ENABLED

資源類型： AWS::CloudTrail::Trail

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cloud-trail-log-file-validation-enabled

檢查是否使用記錄 AWS CloudTrail 建立已簽署的摘要檔。 AWS 建議必須在所有軌跡上啟用檔案驗證。如果驗證為未啟用，則表示規則為「NON_COMPLIANT」。

識別符： CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

資源類型： AWS::CloudTrail::Trail

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cmk-backing-key-rotation-enabled

檢查是否已為每個金鑰啟用自動金鑰輪替，並與客戶建立的 AWS KMS 金鑰的金鑰 ID 相符。如果資源的 AWS Config 記錄程式角色沒有 kms: DescribeKey 權限，則該規則為「不符合」。

> **Note**
>
> 自動金鑰輪換不支援非對稱 KMS 金鑰、HMAC KMS 金鑰、含有匯入金鑰資料的 KMS 金鑰或自訂金鑰存放區中的 KMS 金鑰。

識別符： CMK_BACKING_KEY_ROTATION_ENABLED

資源類型： AWS::KMS::Key

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codebuild-project-artifact-encryption

檢查 AWS CodeBuild 專案是否已為其所有成品啟用加密。如果任何主要或次要 (若有) 成品組態的 'encryptionDisabled' 設定為 'true'，則表示規則為「NON_COMPLIANT」。

識別符：CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

資源類型： AWS::CodeBuild::Project

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codebuild-project-environment-privileged-check

檢查 AWS CodeBuild 項目環境是否啟用了特權模式。如果將「privilegedMode」設置為「真」，則該規則對於 CodeBuild 項目不兼容。

識別符：CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

資源類型： AWS::CodeBuild::Project

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

exemptedProjects (選用), 類型：CSV

以逗號分隔的 CodeBuild 項目名稱列表，這些列表被允許具有「privilegedMode」值為「真」。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codebuild-project-envvar-awscred-check

檢查項目是否包含環境變量 AWS_ACCES_KEY_ID 和 _ 秘密鑰。 AWS當專案環境變數包含純文字憑證，則表示規則為「NON_COMPLIANT」。

標識符：編碼生成 _ 項目 _ ENVVAR_ AWSCRED_CHECK

資源類型： AWS::CodeBuild::Project

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codebuild-project-logging-enabled

檢查 AWS CodeBuild 專案環境是否至少啟用了一個記錄選項。如果目前所有日誌組態的狀態都設定為 'DISABLED'，則表示規則為「NON_COMPLIANT」。

識別符：CODEBUILD_PROJECT_LOGGING_ENABLED

資源類型： AWS::CodeBuild::Project

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

s3 BucketNames (選擇性的), 類型：字串

如果設定 S3 日誌，則應作為日誌傳送目的地之 Amazon S3 儲存貯體名稱的清單 (以逗號分隔)。

雲端 WatchGroupNames (選擇性), 類型：字串

以逗號分隔的 Amazon 日 CloudWatch 誌群組名稱清單，如果設定了日誌，則應將 CloudWatch 日誌傳送至該清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codebuild-project-s3-logs-encrypted

檢查使用 Amazon S3 日誌設定的 AWS CodeBuild 專案是否已為其日誌啟用加密功能。如果在專案的 S3 LogsConfig 中將「加密停用」設定為「真」，則該規則為「不符合 _」。 CodeBuild

識別符：CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

資源類型： AWS::CodeBuild::Project

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

exemptedProjects (選用), 類型：CSV

允許輸出未加密記錄檔的 CodeBuild 專案名稱清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codebuild-project-source-repo-url-check

檢查 Bitbucket 來源儲存庫 URL 是否包含登入憑證。如果 URL 包含任何登入資訊，則表示規則為「NON_COMPLIANT」；如果未包含，則為「COMPLIANT」。

識別符： CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

資源類型： AWS::CodeBuild::Project

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codedeploy-auto-rollback-monitor-enabled

檢查部署群組是否設定了自動部署復原和附加了警示的部署監視。如果或尚未配置 AutoRollbackConfiguration 或 AlarmConfiguration 未啟用，則該規則為「不符合」。

識別符：CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

資源類型： AWS::CodeDeploy::DeploymentGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codedeploy-ec2-minimum-healthy-hosts-configured

檢查 EC2 /內部部署計算平台的部署群組是否設定為使用最小的狀態良好主機機群組百分比，或主機數量大於或等於輸入閾值。如果任一項目低於閾值，則表示規則為「NON_COMPLIANT」。

識別符：CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

資源類型： AWS::CodeDeploy::DeploymentGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

最小值 HealthyHostsFleetPercent (選擇性), 類型：int, 預設：66

部署期間狀態良好主機機群的最小百分比。預設值設為 66%。

最小值 HealthyHostsHostCount (選擇性), 類型：int, 預設：1

部署期間機群中狀態良好主機的最小數量。預設值設定為 1。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codedeploy-lambda-allatonce-traffic-shift-disabled

檢查 Lambda 運算平台的部署群組是否未使用預設部署組態。如果部署群組使用部署組態「預設」，則該規則為「NON_COMPLUTION」CodeDeploy。 LambdaAllAtOnce'.

識別符：CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

資源類型： AWS::CodeDeploy::DeploymentGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codepipeline-deployment-count-check

檢查的第一個部署階段是否 AWS CodePipeline 執行多個部署。可以選擇檢查各個後續剩餘階段部署是否超過指定部署數量 (`deploymentLimit`)。

識別符： CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

資源類型： AWS::CodePipeline::Pipeline

觸發類型： Configuration changes (組態變更)

AWS 區域：只可在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部) 區域使用

參數：

deploymentLimit (選用), 類型：int

各階段可以執行的最大部署數。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## codepipeline-region-fanout-check

檢查 AWS CodePipeline 部署中的每個階段是否超過先前所有組合階段中部署的區域數量的 N 倍以上，其中 N 是區域扇出編號。 AWS CodePipeline 第一部署階段最多可以部署一個區域，而第二部署階段最多可以部署 `regionFanoutFactor` 中指定的最大數量。如果您未提供 `regionFanoutFactor`，預設值為三。例如：如果第一部署階段部署到一個區域，而第二部署階段部署到三個區域，第三部署階段可以部署到 12 個區域，也就是先前階段總和數量乘以區域擴散 (三) 數目。如果部署在第一階段多於一個區域、第二階段多於三個區域，或第三階段多於 12 個區域，則表示規則為 NON_COMPLIANT。

識別符： CODEPIPELINE_REGION_FANOUT_CHECK

資源類型： AWS::CodePipeline::Pipeline

觸發類型： Configuration changes (組態變更)

AWS 區域：只可在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部) 區域使用

參數：

regionFanoutFactor (選擇性), 類型：int, 預設：3

> 在先前所有階段中， AWS CodePipeline 已部署到的區域數目是任何階段可部署到的可接受區域數目。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## custom-eventbus-policy-attached

檢查 Amazon EventBridge 自訂事件匯流排是否附加了以資源為基礎的政策。如果自訂事件匯流排政策沒有連接的資源型政策，則表示規則為「NON_COMPLIANT」。

識別符：CUSTOM_EVENTBUS_POLICY_ATTACHED

資源類型： AWS::Events::EventBus

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## custom-schema-registry-policy-attached

檢查自訂 Amazon EventBridge 架構登錄是否已附加資源政策。針對沒有連接資源政策的自訂結構描述登錄檔，規則為「NON_COMPLIANT」。

識別符：CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

資源類型： AWS::EventSchemas::Registry

觸發類型：定期

AWS 區域: 僅在歐洲 (斯德哥爾摩)、亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、亞太區域 (香港)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (維吉尼亞北部) (雪梨), 加拿大 (中部) 區域

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## cw-loggroup-retention-period-check

檢查 Amazon CloudWatch LogGroup 保留期是否設定為超過 365 天或指定的保留期。如果保留期間小於 (如果指定的話) 或 365 天`MinRetentionTime`，則規則為「NON_ 相容」。

> **Note**
> 如果日誌群組的保留期設定為「永不過期」，則表示規則標示為「COMPLIANT」。

識別符：CW_LOGGROUP_RETENTION_PERIOD_CHECK

資源類型： AWS::Logs::LogGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

LogGroupNames (選擇性), 類型：CSV

用來檢查保留期間的日誌群組名稱清單 (以逗號分隔)。

MinRetentionTime (選擇性), 類型：int

指定保留時間。有效值為：
1、3、5、7、14、30、60、90、120、150、180、365、400、545、731、1827 和 3653。預設保留期間為 365 天。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dax-encryption-enabled

檢查 Amazon DynamoDB Accelerator (DAX) 叢集是否已加密。如果 DAX 叢集未加密，則表示規則為「NON_COMPLIANT」。

識別符：DAX_ENCRYPTION_ENABLED

資源類型： AWS::DAX::Cluster

觸發類型：定期

AWS 區域：僅在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (雪梨) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## Dax-tls 端點加密

檢查您的 Amazon DynamoDB 加速器 (DAX) 叢集是否已 ClusterEndpointEncryptionType 設定為 TLS。如果 DAX 叢集未透過傳輸層安全性 (TLS) 加密，則該規則為「不相容」。

識別碼：DAX_TLS_ 端點 _ 加密

資源類型： AWS::DAX::Cluster

觸發類型：定期

AWS 區域：僅在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (雪梨) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## db-instance-backup-enabled

檢查 RDS 資料庫執行個體是否啟用備份功能。規則會選擇性檢查備份保留期間和備份時間。

識別符： DB_INSTANCE_BACKUP_ENABLED

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

backupRetentionPeriod (選擇性), 類型：int

備份保留期間。

backupRetentionMinimum (選擇性), 類型：int

備份的最低保留期間。

preferredBackupWindow (選擇性), 類型：字串

建立備份的時間範圍。

checkReadReplicas (選擇性), 類型：布林值

檢查 RDS 資料庫執行個體是否啟用讀取複本的備份。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## desired-instance-tenancy

檢查 EC2 執行個體是否有 'tenancy' 值。同時檢查 AMI ID 是否指定要從這些 AMI 啟動，或是否在這些專用執行個體上啟動主機 ID。如果執行個體符合清單中的主機和 AMI (若有指定)，則表示規則為「COMPLIANT」。

識別符： DESIRED_INSTANCE_TENANCY

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

tenancy, 類型：字串

執行個體的必要租用。有效值為 DEDICATED、HOST 和 DEFAULT。

imageId (選用), 類型：CSV

規則只會評估從含指定 ID 之 AMI 啟動的執行個體。以逗號分隔多個 AMI ID。

hostId (選用), 類型：CSV

要啟動之執行個體的 EC2 專用執行個體 ID。以逗號分隔多個主機 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## desired-instance-type

檢查 EC2 執行個體是否為指定的執行個體類型。如果未在參數清單中指定 EC2 執行個體，則表示規則為「NON_COMPLIANT」。如需支援的 EC2 執行個體類型清單，請參閱《適用於 Linux 執行個體的 EC2 使用者指南》中的執行個體類型。

識別符：DESIRED_INSTANCE_TYPE

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

instanceType, 類型：CSV

逗號分隔的 EC2 執行個體類型清單 (例如「t2.small, m4.large, i2.xlarge」)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dms-auto-minor-version-upgrade-check

檢查 AWS Database Migration Service (AWS DMS) 複製執行個體是否已啟用自動次要版本升級。如果 AWS DMS 複製執行個體未設定自動次要版本升級，則規則為「NON_ 相容」。

識別符：DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

資源類型： AWS::DMS::ReplicationInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dms-endpoint-ssl-configured

檢查 AWS Database Migration Service (AWS DMS) 端點是否已設定 SSL 連線。如果 AWS DMS 未設定 SSL 連線，則該規則為「不相容」。

識別符：DMS_ENDPOINT_SSL_CONFIGURED

資源類型： AWS::DMS::Endpoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 啟用 DMS-蒙古 DB-身份驗證

檢查資料倉 AWS 庫的 MongoDb 資料庫移轉服務 (AWS DMS) 端點是否已啟用以密碼為基礎的驗證和存取控制。如果未啟用以密碼為基礎的驗證和存取控制，則該規則為「NON_COLUTION」。

識別碼：DMS_ 蒙古 _ 資料庫驗證 _ 已啟用

資源類型： AWS::DMS::Endpoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## DMS-海王星 IAM 授權啟用

檢查 Amazon Neptune 資料 AWS Database Migration Service (AWS DMS) 端點是否設定了 IAM 授權。如果 Neptune 為目標的 AWS DMS 端點已 IamAuthEnabled 設定為 false，則該規則為「不相容」。

識別碼：DMS _ 海王星 _ 授權 _ 已啟用

資源類型： AWS::DMS::Endpoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 啟用 DMS-雷迪斯

檢查 Redis 資料存放區的資料 AWS Database Migration Service (AWS DMS) 端點是否已啟用與其他端點通訊之資料的 TLS/SSL 加密。如果未啟用 TLS/SSL 加密，則該規則為「不相容」。

識別碼：已啟用 DMS_REDIS_ TLS_

資源類型： AWS::DMS::Endpoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dms-replication-not-public

檢查 AWS Database Migration Service (AWS DMS) 複寫執行個體是否為公用。如果欄位設定為 true，則規則為 PubliclyAccessible 「不相容」。

識別符：DMS_REPLICATION_NOT_PUBLIC

資源類型： AWS::DMS::ReplicationInstance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dms-replication-task-sourcedb-logging

檢查記錄是否已啟用來源資料庫的 AWS DMS 複寫工作的有效嚴重性層級。如果未啟用記錄，或來源資料庫的 DMS 複寫任務的日誌具有無效的嚴重性層級，則表示規則為「NON_COMPLIANT」。

識別符：DMS_REPLICATION_TASK_SOURCEDB_LOGGING

資源類型： AWS::DMS::ReplicationTask

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dms-replication-task-targetdb-logging

檢查目標資料庫的 AWS DMS 複寫工作事件是否已啟用記錄，並具有有效的嚴重性層級。如果未啟用日誌記錄，或目標資料庫複寫任務日誌記錄具有無效的嚴重性層級，則表示規則為「NON_COMPLIANT」。

識別符：DMS_REPLICATION_TASK_TARGETDB_LOGGING

資源類型： AWS::DMS::ReplicationTask

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## docdb-cluster-audit-logging-enabled

檢查 Amazon 文件資料庫 (與 MongoDB 相容性) 執行個體叢集是否已啟用稽核 CloudWatch 日誌的記錄匯出功能。如果 Amazon DocumentDB 執行個體叢集沒有為稽核日誌啟用 CloudWatch 日誌匯出，則該規則為「不符合 _ 規範」。

識別符：DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：只可在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、歐洲 (米蘭)、亞太區域 (東京)、美國西部 (奧勒岡)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部)、中國 (寧夏) 區域使用

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## docdb-cluster-backup-retention-check

檢查 Amazon Document DB 叢集保留期間是否設定為特定天數。如果保留期間小於參數指定的值，則表示規則為「NON_COMPLIANT」。

識別符：DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：只可在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、歐洲 (米蘭)、亞太區域 (東京)、美國西部 (奧勒岡)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部)、中國 (寧夏) 區域使用

參數：

最小值 BackupRetentionPeriod (選擇性), 類型：int

> 備份最少應保留的天數。有效值為 1 到 35，預設值為 7。如果值大於「備份」，則此規則為「不相容」RetentionPeriod。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## docdb-cluster-deletion-protection-enabled

檢查 Amazon DocumentDB (with MongoDB compatibility) 叢集是否已啟用刪除保護。如果 Amazon DocumentDB 叢集的 deletionProtection 欄位設定為 false，則表示規則為「NON_COMPLIANT」。

識別符：DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：只可在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、歐洲 (米蘭)、亞太區域 (東京)、美國西部 (奧勒岡)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部)、中國 (寧夏) 區域使用

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## docdb-cluster-encrypted

檢查 Amazon DocumentDB (with MongoDB compatibility) 叢集是否已啟用儲存加密。如果未啟用儲存加密，則表示規則為「NON_COMPLIANT」。

識別符：DOCDB_CLUSTER_ENCRYPTED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：只可在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、歐洲 (米蘭)、亞太區域 (東京)、美國西部 (奧勒岡)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部)、中國 (寧夏) 區域使用

參數：

kmsKeyArns (選擇性), 類型：CSV

以逗號分隔的 KMS 金鑰 ARN 清單，可與加密叢集的 KmsKey識別碼進行比較。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## docdb-cluster-snapshot-public-prohibited

檢查 Amazon DocumentDB 手動叢集快照是否為公有狀態。如果任何 Amazon DocumentDB 手動叢集快照為公有狀態，則表示規則為「NON_COMPLIANT」。

識別符：DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

資源類型:AWS:: RDS:: 資料庫 ClusterSnapshot

觸發類型： Configuration changes (組態變更)

AWS 區域：只可在亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、歐洲 (米蘭)、亞太區域 (東京)、美國西部 (奧勒岡)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部) 區域使用

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-autoscaling-enabled

檢查 Amazon DynamoDB 資料表或全域次要索引是否可以使用隨需模式或已啟用自動擴展的佈建模式來處理讀取/寫入容量。如果在未啟用自動擴展的情況下使用任一模式，則表示規則為「NON_COMPLIANT」

識別符： DYNAMODB_AUTOSCALING_ENABLED

資源類型： AWS::DynamoDB::Table

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

分鐘ProvisionedReadCapacity （可選），類型：int

應該在 Auto Scaling 群組中對讀取容量佈建的最小單位數。

最大ProvisionedReadCapacity （可選），類型：int

應該在 Auto Scaling 群組中對讀取容量佈建的最大單位數。

targetReadUtilization (選擇性), 類型：double

讀取容量的目標使用率百分比。目標使用率是以使用容量/佈建容量的比率來表示。

分鐘ProvisionedWriteCapacity （可選），類型：int

應該在 Auto Scaling 群組中對寫入容量佈建的最小單位數。

最大ProvisionedWriteCapacity （可選），類型：int

應該在 Auto Scaling 群組中對寫入容量佈建的最大單位數。

targetWriteUtilization (選擇性), 類型：double

寫入容量的目標使用率百分比。目標使用率是以使用容量/佈建容量的比率來表示。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-in-backup-plan

檢查 B AWS ackup 計劃中是否存在 Amazon DynamoDB 表格。如果 Amazon DynamoDB 表格不存在於任何 Backup 計劃中，則該規則為「不符合 _ 規範」。 AWS

識別符：DYNAMODB_IN_BACKUP_PLAN

資源類型： AWS::DynamoDB::Table

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-last-backup-recovery-point-created

檢查是否在指定期間內為 Amazon DynamoDB 資料表建立復原點。如果 DynamoDB 資料表沒有在指定期間內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::DynamoDB::Table

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 DynamoDB 資料表標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 DynamoDB 資料表名稱。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-meets-restore-time-target

確認 Amazon DynamoDB 資料表的還原時間是否符合指定的持續時間。如果 DynamoDB 表格 LatestRestoreExecutionTimeMinutes 大於分鐘，則該規則為「不符合 _」。 maxRestoreTime

識別碼：DYNAMODB_MEETS_RESTORE_TIME_TARGET

資源類型： AWS::DynamoDB::Table

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 DynamoDB 資料表標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則要檢查的 DynamoDB 資料表名稱。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-pitr-enabled

檢查 Amazon DynamoDB 資料表是否已啟用 point-in-time 復原 (PITR)。如果 DynamoDB 資料表未啟用 PITR，則表示規則為「NON_COMPLIANT」。

識別碼：DYNAMODB_PITR_ENABLED

資源類型： AWS::DynamoDB::Table

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-resources-protected-by-backup-plan

檢查 Amazon DynamoDB 資料表是否受備份計畫保護。如果備份計畫未涵蓋 DynamoDB 資料表，則表示規則為「NON_COMPLIANT」。

識別符：DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::DynamoDB::Table

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 DynamoDB 資料表標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 DynamoDB 資料表名稱。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-table-deletion-protection-enabled

檢查 Amazon DynamoDB 資料表是否已將刪除保護設為啟用。如果資料表的刪除保護設為停用，則表示規則為「NON_COMPLIANT」。

識別符：DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

資源類型： AWS::DynamoDB::Table

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-table-encrypted-kms

檢查 Amazon DynamoDB 資料表是否已使用金 AWS 鑰管理服務 (KMS) 加密。如果 Amazon DynamoDB 資料表未使用 KMS 加密，則該規則為「不符合 _」標準。 AWS 如果加密的 AWS KMS 金鑰不存在於`kmsKeyArns`輸入參數中，則該規則也是「不符合 _ 規範」。

識別碼：DYNAMODB_TABLE_ENCRYPTED_KMS

資源類型： AWS::DynamoDB::Table

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：CSV

允許以逗號分隔的 AWS KMS 金鑰 ARN 清單來加密 Amazon DynamoDB 資料表。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-table-encryption-enabled

檢查 Amazon DynamoDB 資料表是否已加密，並檢查其狀態。如果欄位狀態為啟用或啟用中，則表示規則為 COMPLIANT。

Identifier: (識別符：) DYNAMODB_TABLE_ENCRYPTION_ENABLED

資源類型： AWS::DynamoDB::Table

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## dynamodb-throughput-limit-check

檢查佈建的 DynamoDB 輸送量是否接近帳戶的上限。規則預設會檢查佈建的輸送量是否超過帳戶上限的 80% 閾值。

識別符： DYNAMODB_THROUGHPUT_LIMIT_CHECK

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

帳戶管理 (選擇性ThresholdPercentage ), 類型：int, 預設：80

帳戶佈建的讀取容量單元百分比。達到此數值時，規則將標示為未合規。

帳戶管理 (可選ThresholdPercentage ), 類型：int, 預設：80

帳戶佈建的寫入容量單元百分比。達到此數值時，規則將標示為未合規。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ebs-in-backup-plan

檢查 Backup 計劃中是否已新增 Amazon 彈性區塊存放區 (Amazon EBS) 磁碟區。 AWS 如果 Amazon EBS 磁碟區未包含在備份計畫中，則表示規則為「NON_COMPLIANT」。

識別符：EBS_IN_BACKUP_PLAN

資源類型： AWS::EC2::Volume

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ebs-last-backup-recovery-point-created

檢查是否已為 Amazon Elastic Block Store (Amazon EBS) 建立復原點。如果 Amazon EBS 磁碟區沒有在指定期間內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::EC2::Volume

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon EBS 磁碟區標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 Amazon EBS 磁碟區 ID。

恢復PointAgeValue（可選），類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit（可選），類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ebs-meets-restore-time-target

確認 (Amazon Elastic Block Store (Amazon EBS) 磁碟區的還原時間是否符合指定的持續時間。如果 Amazon EBS 磁碟區大於 LatestRestoreExecutionTimeMinutes 分鐘，則該規則為「不相容」。maxRestoreTime

識別碼：EBS_MEETS_RESTORE_TIME_TARGET

資源類型： AWS::EC2::Volume

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 Amazon EBS 磁碟區的標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則要檢查的 Amazon EBS 磁碟區 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ebs-optimized-instance

檢查是否已針對可進行 Amazon EBS 最佳化的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體進行 Amazon EBS 最佳化。如果沒有針對可進行 EBS 最佳化的 Amazon EC2 執行個體啟用 EBS 最佳化，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> EBS 最佳化的 EC2 執行個體預設會一律導致規則評估傳回 `COMPLIANT`。

識別符： EBS_OPTIMIZED_INSTANCE

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ebs-resources-protected-by-backup-plan

檢查 Amazon Elastic Block Store (Amazon EBS) 磁碟區是否受備份計畫保護。如果備份計畫未涵蓋 Amazon EBS 磁碟區，則表示規則為「NON_COMPLIANT」。

識別符：EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::EC2::Volume

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon EBS 磁碟區的標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 Amazon EBS 磁碟區 ID。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ebs-snapshot-public-restorable-check

檢查 Amazon Elastic Block Store (Amazon EBS) 快照是否不可公開還原。如果將一個或多個具有 RestorableByUserIds 欄位的快照設定為「全部」(也就是說，Amazon EBS 快照為公用)，則該規則為「不合規」。

識別符： EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-client-vpn-connection-log-enabled

檢查 AWS Client VPN 端點是否已啟用用戶端連線記錄。如果「配置」，則該規則為「不符合 _」。ConnectionLog選項。啟用 '被設置為假。

識別符：EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

資源類型: AWS::EC2::ClientVpn端點

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-client-vpn-not-authorize-all

檢查 AWS Client VPN 授權規則是否授權所有用戶端的連線存取。如果 " 存在且設定為 true，則此規則為 AccessAll「不相容」。

識別符：EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

資源類型: AWS::EC2::ClientVpn端點

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-ebs-encryption-by-default

檢查是否預設啟用 Amazon Elastic Block Store (EBS) 加密。如果加密未啟用，則表示規則為「NON_COMPLIANT」。

識別碼：EC2_EBS_ENCRYPTION_BY_DEFAULT

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-imdsv2-check

檢查 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料版本是否已設定執行個體中繼資料服務第 2 版 (IMDSv2)。如果設定為選用規則，則該規則 HttpTokens 為「不相容」。

識別符：EC2_IMDSV2_CHECK

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-instance-detailed-monitoring-enabled

檢查 EC2 執行個體是否啟用詳細監控。如果未啟用詳細監控，則表示規則為「NON_COMPLIANT」。

識別符： EC2_INSTANCE_DETAILED_MONITORING_ENABLED

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-instance-managed-by-systems-manager

> **Important**
>
> 針對此規則，規則識別符 (EC2_INSTANCE_MANAGED_BY_SSM) 和規則名稱 (ec2-instance-managed-by-systems-manager) 不同。

檢查您的 Amazon EC2 執行個體是否由 AWS Systems Manager 代理程式 (SSM 代理程式) 管理。如果 EC2 執行個體正在執行且 SSM 代理程式停止，或者 EC2 執行個體正在執行且 SSM 代理程式終止，則該規則為「不符合」規則。

> **Note**
>
> 如果 EC2 執行個體停止且 SSM 代理程式正在執行，則規則不會傳回「非符合規範」。

識別符：EC2_INSTANCE_MANAGED_BY_SSM

資源型態： AWS::EC2::Instance, AWS::SSM::ManagedInstance庫存管理

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-instance-multiple-eni-check

檢查 Amazon Elastic Compute Cloud (Amazon EC2) 是否使用多個彈性網路介面 (ENI) 或 Elastic Fabric Adapter (EFA)。如果 Amazon EC2 執行個體使用多個網路介面，則表示規則為「NON_COMPLIANT」。

識別符：EC2_INSTANCE_MULTIPLE_ENI_CHECK

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

NetworkInterfaceIds (選擇性), 類型：CSV

以逗號分隔的網路執行個體 ID 清單

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-instance-no-public-ip

檢查 EC2 執行個體是否擁有公有 IP 關聯。如果 publicIp 欄位出現在 EC2 執行個體組態項目，則表示規則為「NON_COMPLIANT」。此規則僅適用於 IPv4。

內容：公有 IP 地址可以讓您直接從網際網路存取 EC2 執行個體，從安全或合規的角度來看，這可能並不一定是必要的：

- 安全性：在許多情況下，除非需要公開存取，否則您可能不希望 EC2 執行個體擁有公有 IP 地址。擁有公有 IP 地址可能會使 EC2 執行個體面臨潛在的安全風險，例如未經授權的存取或攻擊。
- 合規性：各種合規性標準 (例如 PCI、DSS 或 HIPAA) 在網路分隔和存取控制方面都有特定要求。確保 EC2 執行個體沒有不必要的公有 IP 地址，有助於確保符合這些要求。
- 成本管理：公有 IP 地址可能會產生額外費用，尤其是在有 EC2 執行個體持續關聯的情況下。您可以透過識別不需要公有 IP 的 EC2 執行個體來降低成本。

識別符： EC2_INSTANCE_NO_PUBLIC_IP

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-instance-profile-attached

檢查 EC2 執行個體是否附加了 AWS Identity and Access Management (IAM) 設定檔。如果 EC2 執行個體沒有連接 IAM 設定檔，則表示規則為「NON_COMPLIANT」。

識別符：EC2_INSTANCE_PROFILE_ATTACHED

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

IamInstanceProfileArnList (選擇性), 類型：CSV

可附加至 Amazon EC2 執行個體的 IAM 設定檔 Amazon Resource Name (ARN) 清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-last-backup-recovery-point-created

檢查 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體是否已建立復原點。如果 Amazon EC2 執行個體沒有在指定期間內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::EC2::Instance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon EC2 執行個體標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 Amazon EC2 執行個體 ID。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-launch-template-public-ip-disabled

檢查 Amazon EC2 啟動範本是否設定為將公有 IP 地址指派給網路介面。如果 EC2 啟動範本的預設版本至少有 1 個網路介面且 " 設定為 'true AssociatePublicIpAddress'，則該規則為「不符合」。

識別符：EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

資源類型： AWS::EC2::LaunchTemplate

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

exemptedLaunchTemplates (選擇性), 類型：CSV

以逗號分隔的豁免 EC2 啟動範本 ID 清單，這些 ID 允許使網路界面的 AssociatePublicIpAddress 值設定為 'true'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-managedinstance-applications-blacklisted

檢查執行個體上是否未安裝任何指定的應用程式。可選擇性指定版本。較新的版本將不會被拒絕列出。可選擇性指定平台只將規則套用到執行該平台的執行個體。

識別符： EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

資源型態： AWS::SSM::ManagedInstance庫存管理

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

applicationNames, 類型：CSV

逗號分隔的應用程式名稱清單。可選擇性指定附加 ':' 的版本 (例如 'Chrome:0.5.3, Firefox')。

> **Note**
>
> 應用程式名稱必須完全相符。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用 **`firefox-compat`**。此外，目前 AWS Config 不支援 applicationNames 稱參數的萬用字元 (例如)。**`firefox*`**

platformType (選用), 類型：字串

平台類型 (例如 'Linux' 或 'Windows')。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-managedinstance-applications-required

檢查執行個體上是否已安裝所有指定的應用程式。可選擇性指定最低可接受的版本。您也可以指定平台只將規則套用到執行該平台的執行個體。

> **Note**
>
> 確保在 EC2 執行個體上執行 SSM 代理程式，並建立收集應用程式軟體庫存的關聯。如果尚未安裝 SSM 代理程式或尚未建立或執行關聯，則規則會傳回「NON_COMPLIANT」。

識別符： EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

資源型態： AWS::SSM::ManagedInstance庫存管理

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

applicationNames, 類型：CSV

逗號分隔的應用程式名稱清單。可選擇性指定附加 ':' 的版本 (例如 'Chrome:0.5.3, Firefox')。

> **Note**
>
> 應用程式名稱必須完全相符。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用 **`firefox-compat`**。此外，目前 AWS Config 不支援 applicationNames 稱參數的萬用字元 (例如)。**`firefox*`**

platformType (選用), 類型：字串

平台類型 (例如 'Linux' 或 'Windows')。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-managedinstance-association-compliance-status-check

在執行個體上執行關聯之後，檢查「 AWS Systems Manager」關聯符合性的狀態是否為「相容」或「非相容」。如果欄位狀態是 COMPLIANT，表示規則合規。如需關聯的詳細資訊，請參閱《什麼是關聯？》。

識別符： EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

資源類型： AWS::SSM::AssociationCompliance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-managedinstance-inventory-blacklisted

檢查 Amazon EC2 Systems Manager 所管理的執行個體是否設定為收集黑名單庫存類型。

識別符： EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

資源型態： AWS::SSM::ManagedInstance存貨

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

inventoryNames, 類型：CSV

以逗號分隔的 Systems Manager 庫存類型清單 (例如，': 網路AWS,: AWS'WindowsUpdate)。

platformType (選用), 類型：字串

平台類型 (例如 'Linux')。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-managedinstance-patch-compliance-status-check

在執行個體上安裝修補程式後，檢查 AWS Systems Manager 修補程式符合性的符合性狀態是否為「相容」或「非符合」。如果欄位狀態是 COMPLIANT，表示規則合規。

識別符： EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

資源類型： AWS::SSM::PatchCompliance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-managedinstance-platform-check

檢查 EC2 受管執行個體是否擁有所要的組態。

識別符： EC2_MANAGEDINSTANCE_PLATFORM_CHECK

資源型態： AWS::SSM::ManagedInstance庫存管理

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

platformType, 類型：字串

平台類型 (例如 'Linux')。

platformVersion (選用), 類型：字串

平台版本 (例如 '2016.09')。

agentVersion (選用), 類型：字串

代理程式版本 (例如 '2.0.433.0')。

platformName (選用), 類型：字串

平台的版本 (例如 '2016.09')。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-meets-restore-time-target

確認 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的還原時間是否符合指定的持續時間。如果 Amazon EC2 執行個體 LatestRestoreExecutionTimeMinutes 的時間大於 maxRestoreTime 分鐘，則該規則為「不符合」規則。

識別碼：EC2_MEETS_RESTORE_TIME_TARGET

資源類型： AWS::EC2::Instance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 Amazon EC2 執行個體標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則要檢查的 Amazon EC2 執行個體 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-no-amazon-key-pair

檢查執行中的 Amazon Elastic Compute Cloud (EC2) 執行個體是否使用 Amazon 金鑰對啟動。如果使用金鑰對啟動執行中的 EC2 執行個體，則表示規則為「NON_COMPLIANT」。

識別符：EC2_NO_AMAZON_KEY_PAIR

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-paravirtual-instance-check

檢查 EC2 執行個體的虛擬化類型是否為半虛擬化。如果將 'virtualizationType' 設定為 'paravirtual'，則表示 EC2 執行個體的此規則為「NON_COMPLIANT」。

識別符：EC2_PARAVIRTUAL_INSTANCE_CHECK

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在中國 (北京)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (雪梨) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-resources-protected-by-backup-plan

檢查 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體是否受備份計畫保護。如果備份計畫未涵蓋 Amazon EC2 執行個體，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則僅適用於執行中的 Amazon EC2 執行個體，不適用於已關閉的執行個體。

識別符：EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::EC2::Instance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon EC2 執行個體標籤 (採用 JSON 格式 `{"tagkey" : "tagValue"}`)。

resourceId (選用), 類型：字串

規則要檢查的 Amazon EC2 執行個體 ID。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-security-group-attached-to-eni

檢查非預設安全群組是否連接至彈性網路介面。如果安全群組未與網路介面建立關聯，則表示規則為「NON_COMPLIANT」。

識別符： EC2_SECURITY_GROUP_ATTACHED_TO_ENI

資源類型： AWS::EC2::SecurityGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-security-group-attached-to-eni-periodic

檢查非預設安全群組是否已連接至彈性網絡介面 (ENI)。如果安全群組未與 ENI 建立關聯，則表示規則為「NON_COMPLIANT」。不屬於呼叫帳戶的安全性群組會評估為「NOT_APPLICABLE」。

> **Note**
>
> 此規則會報告 `AWS::EC2::SecurityGroup` 資源類型。但是，為了使規則有效執行，您必須啟用 `AWS::EC2::NetworkInterface` 資源類型的記錄功能。

識別符：EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

資源類型： AWS::EC2::SecurityGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-stopped-instance

檢查 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的停止時間是否超過允許的天數。如果 Amazon EC2 執行個體狀態的停止時間已超過允許的天數，或天數無法判斷，則表示規則為「NON_COMPLIANT」。

識別符：EC2_STOPPED_INSTANCE

資源類型： AWS::EC2::Instance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

AllowedDays (選擇性), 類型：int, 預設：30

在規則為「NON_COMPLIANT」之前，Amazon EC2 執行個體可以停止的天數。預設天數為 30。

> **Note**
>
> 因為此規則依賴於所收集的歷史資料，所以選取的天數必須少於設定的保留期間。如需有關歷史資料保留的詳細資訊，請參閱刪除資 AWS Config 料。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-token-hop-limit-check

檢查 Amazon Elastic Compute Cloud (EC2) 執行個體中繼資料是否具有低於所需限制的指定字符跳轉限制。如果執行個體的跳轉限制值超過預期限制，則表示執行個體的規則為「NON_COMPLIANT」。

識別符：EC2_TOKEN_HOP_LIMIT_CHECK

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

tokenHopLimit (選擇性), 類型：int

所需的字符跳轉限制。有效值介於 1 到 64 之間。如未指定參數，則預設值為 1。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-transit-gateway-auto-vpc-attach-disabled

檢查亞馬遜彈性運算雲端 (Amazon EC2) 傳輸閘道是否已啟用 AutoAccept SharedAttachments "。如果將「」設定為「啟用」，則 Transit Gateway 的規則為 AutoAccept SharedAttachments「不符合」規則。

識別符：EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

資源類型： AWS::EC2::TransitGateway

觸發類型： Configuration changes (組態變更)

AWS 區域: 僅適用於歐洲 (斯德哥爾摩)、歐洲 (巴黎)、美國東部 (俄亥俄)、非洲 (開普敦)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、歐洲 (米蘭)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利福尼亞)、歐洲 (倫敦)、歐洲 (米蘭)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利福尼亞)、亞太區域 (北加利福尼亞)、), 加拿大 (中部) 區域

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-volume-inuse-check

檢查 EBS 磁碟區是否連接至 EC2 執行個體。也可選擇性檢查 EBS 磁碟區是否在執行個體終止時標記為刪除。

如果 EBS 磁碟區連接到執行中的 EC2 執行個體，則表示規則為「COMPLIANT」。在這種情況下，當 EC2 執行個體正在主動使用 EBS 磁碟區時，則表示其為「COMPLIANT」。

如果 EBS 磁碟區未連接到任何 EC2 執行個體，或連接到已停止或終止的 EC2 執行個體，則表示規則為「NON_COMPLIANT」。在這種情況下，當 EC2 執行個體未主動使用 EBS 磁碟區時，則表示其為「NON_COMPLIANT」。

識別符： EC2_VOLUME_INUSE_CHECK

資源類型： AWS::EC2::Volume

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

deleteOnTermination (選擇性), 類型：布林值

> EBS 磁碟區會在執行個體終止時標記為刪除。可能的值：True 或 False (其他輸入值標記為「NON_COMPLIANT」)。如果設定為 `True`，則如果終止的 EBS 磁碟區未標示為要刪除，則表示規則為「NON_COMPLIANT」。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecr-private-image-scanning-enabled

檢查私有 Amazon Elastic Container Registry (Amazon ECR) 儲存庫是否已啟用映像掃描。
如果私用 Amazon ECR 儲存庫的掃描頻率未設定為在推送或連續掃描時掃描，則表示規則為「NON_COMPLIANT」。如需映像掃描的詳細資訊，請參閱《Amazon ECR 使用者指南》中的映像掃描。

識別符：ECR_PRIVATE_IMAGE_SCANNING_ENABLED

資源類型： AWS::ECR::Repository

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecr-private-lifecycle-policy-configured

檢查私有 Amazon Elastic Container Registry (ECR) 儲存庫是否已設定至少一個生命週期政策。如果沒有為 ECR 私有儲存庫設定生命週期原則，則表示規則為「NON_COMPLIANT」。

識別符：ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

資源類型： AWS::ECR::Repository

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecr-private-tag-immutability-enabled

檢查私有 Amazon Elastic Container Registry (ECR) 儲存庫是否已啟用標籤不變性。如果未為私有 ECR 儲存庫啟用標籤不變性，則表示規則為「NON_COMPLIANT」。

識別符：ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

資源類型： AWS::ECR::Repository

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-awsvpc-networking-enabled

檢查活動 ECS 的網絡模式是否設置TaskDefinitions 為 'awsvpc'。如果使用中 ECS 未設定為「awsvpc」，則此規則TaskDefinitions 為「不相容」。

> **Note**
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別碼：ECS_ 已啟AWSVPC_NETWORKING用

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-containers-nonprivileged

檢查 ECS 的容器定義中的特權參數TaskDefinitions 是否設置為 'true'。如果權限參數為 ‘true’，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別符：ECS_CONTAINERS_NONPRIVILEGED

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-containers-readonly-access

檢查 Amazon Elastic Container Service (Amazon ECS) 容器是否只對其根檔案系統具有唯讀存取權。如果 ECS 容器定義中的 readonlyRootFilesystem 參數設定為「假」，則規則TaskDefinitions 為「不相容」。

> **Note**
>
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別符：ECS_CONTAINERS_READONLY_ACCESS

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-container-insights-enabled

檢查 Amazon Elastic Container Service 叢集是否已啟用容器洞察功能。如果未啟用容器洞察功能，則表示規則為「NON_COMPLIANT」。

識別符：ECS_CONTAINER_INSIGHTS_ENABLED

資源類型： AWS::ECS::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-fargate-latest-platform-version

檢查 ECS Fargate 服務是否設定為最新的平台版本。如果 Fargate 啟動類型未設定 PlatformVersion 為 LATEST，或者既未提供 latestLinuxVersion 也`latestWindowsVersion`未作為參數提供，則該規則為「非 _ 相容」。

識別符：ECS_FARGATE_LATEST_PLATFORM_VERSION

資源類型： AWS::ECS::Service

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

latestLinuxVersion (選擇性), 類型：字串

最新的 Linux 支援語意版本控制 (SemVer) 格式的 PlatformVersion "。如果已部署 Fargate 且已明確指定或使用 PlatformVersion " 作為 "DeploymentController， CodeDeploy 則可能需要參數

latestWindowsVersion (選擇性), 類型：字串

最新的視窗支援語意版本控制 (SemVer) 格式的 PlatformVersion "。如果已部署 Fargate 且已明確指定或使用 PlatformVersion " 作為 "DeploymentController， CodeDeploy 則可能需要參數

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-no-environment-secrets

檢查密碼是否作為容器環境變數傳遞。如果一或多個環境變數金鑰與 'secretKeys' 參數中列出的金鑰相符 (不包括來自其他位置 (例如 Amazon S3) 的環境變數)，則表示規則為「NON_COMPLIANT」。

> **Note**
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別符：ECS_NO_ENVIRONMENT_SECRETS

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

secretKeys, 類型：CSV

要在「任務定義」內容器定義之環境變數中搜尋的金鑰名稱清單 (以逗號分隔)。多餘的空格將被刪除。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-task-definition-log-configuration

檢查是否已在作用中的 ECS 任務定義上設定 logConfiguration。如果使用中 ECS 沒有定義記錄組態資源，或者至TaskDefinition 少一個容器定義中記錄組態的值為空，則此規則為 NON_COMPLUTION。

> **Note**
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別符：ECS_TASK_DEFINITION_LOG_CONFIGURATION

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-task-definition-memory-hard-limit

檢查 Amazon Elastic Container Service (ECS) 任務定義是否為其容器定義設定記憶體限制。如果其中一個容器定義沒有 'memory' 參數，則表示任務定義的規則為「NON_COMPLIANT」。

> **Note**
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別符：ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-task-definition-nonroot-user

檢查 ECS 是否為要在其上執行的 Amazon Elastic Container Service (Amazon ECS) EC2 啟動類型容器TaskDefinitions 指定使用者。如果 'user' 參數不存在或設定為 'root'，則表示規則為「NON_COMPLIANT」。

> **Note**
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別符：ECS_TASK_DEFINITION_NONROOT_USER

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-task-definition-pid-mode-check

檢查 ECS TaskDefinitions 是否設定為與其 Amazon Elastic Container Service (Amazon ECS) 容器共用主機的程序命名空間。如果 pidMode 參數設定為 'host'，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則只會評估 Amazon ECS 任務定義的最新使用中修訂。

識別符：ECS_TASK_DEFINITION_PID_MODE_CHECK

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ecs-task-definition-user-for-host-mode-check

檢查 `NetworkMode` 已設定為主機的最新作用中 Amazon Elastic Container Service (Amazon ECS) 任務定義中是否有未經授權的許可。若 `NetworkMode` 設定為主機、`privileged` 容器定義設為 false 或空白，且 `user` 設定為根或空白的任務定義，則規則為「NON_COMPLIANT」。

> **Important**
>
> 建議您從 Amazon ECS 任務定義中移除提升的權限。當`privileged`為 true 時，容器會在主機容器執行個體上獲得提升的權限 (類似於`root`使用者)。執行使用 `host` 網路模式的任務時，為了獲得更好的安全性，不要使用根使用者 (UID 0) 執行容器。作為最佳安全實務，請一律使用非根使用者。

識別符：ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

資源類型： AWS::ECS::TaskDefinition

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

SkipInactiveTaskDefinitions (選擇性), 類型：布林值

> 不檢查非作用中 Amazon EC2 任務定義的布林值標記。如果設定為 'true'，則規則不會評估非作用中的 Amazon EC2 任務定義。如果設定為 'false'，則規則將評估非作用中 Amazon EC2 任務定義的最新修訂。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs-access-point-enforce-root-directory

檢查 Amazon Elastic File System (Amazon EFS) 存取點是否設定為強制執行根目錄。如果 'Path' 的值設定為 '/' (檔案系統的預設根目錄)，則表示規則為「NON_COMPLIANT」。

識別符：EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

資源類型： AWS::EFS::AccessPoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

approvedDirectories (選用), 類型：CSV

核准用於 Amazon EFS 存取點根目錄強制執行的子目錄路徑清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs-access-point-enforce-user-identity

檢查 Amazon Elastic File System (Amazon EFS) 存取點是否設定為強制執行使用者身分。如果未定義 'PosixUser' 或提供參數且對應參數中沒有相符項，則規則為「NON_COMPLUTION」。

識別符：EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

資源類型： AWS::EFS::AccessPoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

approvedUids (選用), 類型：CSV

已核准用於 EFS 存取點使用者強制執行的 POSIX 使用者 ID 清單 (以逗號分隔)。

approvedGids (選用), 類型：CSV

已核准用於 EFS 存取點使用者強制執行的 POSIX 群組 ID 清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs-encrypted-check

檢查 Amazon Elastic File System (Amazon EFS) 是否設定為使用 AWS Key Management Service (AWS KMS) 加密檔案資料。如果加密金鑰在 `DescribeFileSystems` 上設為 false，或 `KmsKeyId` 上的金鑰 `DescribeFileSystems` 不符合 `KmsKeyId` 參數，則表示規則為 NON_COMPLIANT。

識別符： EFS_ENCRYPTED_CHECK

資源類型： AWS::EFS::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

KmsKeyId (選擇性), 類型：字串

用於加密 EFS 檔案系統之 KMS 金鑰的 Amazon Resource Name (ARN)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs-in-backup-plan

檢查 Amazon Elastic File System (Amazon EFS) 檔案系統是否已新增至 Backup 的備 AWS 份計劃。如果備份計畫未涵蓋 EFS 檔案系統，則表示規則為「NON_COMPLIANT」。

識別符：EFS_IN_BACKUP_PLAN

資源類型： AWS::EFS::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs-last-backup-recovery-point-created

檢查是否已為 Amazon Elastic File System (Amazon EFS) 建立復原點。如果 Amazon EFS 檔案系統沒有在指定期間內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::EFS::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon EFS 檔案系統標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則中需檢查的 EFS 檔案系統 ID。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs-meets-restore-time-target

確認 Amazon Elastic File System (Amazon EFS) 檔案系統的還原時間是否符合指定的持續時間。如果 Amazon EFS 檔案系統的時間超 maxRestoreTime 過 LatestRestoreExecutionTimeMinutes 分鐘，則該規則為「不符合 _」標準。

識別碼：EFS_MEETS_RESTORE_TIME_TARGET

資源類型： AWS::EFS::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 Amazon EFS 檔案系統標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則中需檢查的 EFS 檔案系統 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs 掛載目標-公共可訪問

檢查 Amazon Elastic File System (Amazon EFS) 掛載目標是否與公有子網路沒有關聯。如果 Amazon EFS 掛載目標與公有子網路相關聯，則該規則為「不合規」。

識別碼：EF_ 掛載目標 _ 公用 _ 可存取

資源類型： AWS::EFS::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## efs-resources-protected-by-backup-plan

檢查 Amazon Elastic File System (Amazon EFS) 是否受備份計畫的保護。如果備份計畫未涵蓋 EFS 檔案系統，則表示規則為「NON_COMPLIANT」。

識別符：EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::EFS::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 EFS 檔案系統標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 EFS 檔案系統 ID。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選），類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eip-attached

檢查分配給 AWS 帳戶的所有彈性 IP 地址是否連接到 EC2 執行個體或使用中的彈性網路界面。如果彈性 IP 位址的 'AssociationId' 為空，則該規則為 NON_ 相容。

> **Note**
>
> 評估發生之後，可能需要長達 6 小時後才能使用結果。

識別符： EIP_ATTACHED

資源類型：AWS::EC2::EIP

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COMPANTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
```

```
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eks-cluster-logging-enabled

檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集是否已設定為已啟用日誌記錄。如果未針對所有日誌類型啟用 Amazon EKS 叢集的記錄功能，則表示規則為「NON_COMPLIANT」。

識別符：EKS_CLUSTER_LOGGING_ENABLED

資源類型： AWS::EKS::Cluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eks-cluster-log-enabled

檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集是否已設定為已啟用日誌記錄。如果未啟用 Amazon EKS 叢集的日誌記錄，或未使用所述的日誌類型啟用日誌記錄，則表示規則為「NON_COMPLIANT」。

識別符：EKS_CLUSTER_LOG_ENABLED

資源類型： AWS::EKS::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

logTypes (選用), 類型：CSV

應啟用的 EKS 叢集控制平面日誌類型清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eks-cluster-oldest-supported-version

檢查 Amazon Elastic Kubernetes Service (EKS) 叢集是否正在執行最舊的支援版本。如果 EKS 叢集正在執行最舊的支援版本 (等於參數 '`oldestVersionSupported`')，則表示規則為「NON_COMPLIANT」。

識別符：EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

資源類型： AWS::EKS::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

最古老 VersionSupported, 類型：字串

AWS上支援的 Kubernetes 最舊版本值。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eks-群集秘密加密

檢查 Amazon EKS 叢集是否設定為使用 KMS 加密的 Kubernetes 密碼。 AWS 如果 EKS 叢集沒有加密配置資源，或者如果加密配置未將密碼命名為資源，則該規則為「不相容」。

識別碼：EK_ 叢集 _ 秘密加密

資源類型： AWS::EKS::Cluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：CSV

已核准用於 EKS 使用的 KMS 金鑰 Amazon 資源名稱 (ARN) 的逗號分隔清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eks-cluster-supported-version

檢查 Amazon Elastic Kubernetes Service (EKS) 叢集是否正在執行受支援的 Kubernetes 版本。如果 EKS 叢集正在執行不受支援的版本 (小於參數 '`oldestVersionSupported`')，則表示此規則為「NON_COMPLIANT」。

識別符：EKS_CLUSTER_SUPPORTED_VERSION

資源類型： AWS::EKS::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

最古老 VersionSupported, 類型：字串

AWS上支援的 Kubernetes 最舊版本值。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eks-endpoint-no-public-access

檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 端點是否無法公開存取。如果端點可公開存取，則表示規則為「NON_COMPLIANT」。

識別符：EKS_ENDPOINT_NO_PUBLIC_ACCESS

資源類型： AWS::EKS::Cluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## eks-secrets-encrypted

檢查 Amazon Elastic Kubernetes Service 叢集是否設定為使用 (KMS) 金鑰加密 Kubernetes 密碼。AWS Key Management Service

- 如果 EKS 叢集具有 encryptionConfig 作為其中一個資源的密碼，則表示規則為「NON_COMPLIANT」。
- 如果用於加密 EKS 密碼的金鑰與參數相符，則表示規則也是「COMPLIANT」。
- 如果 EKS 叢集沒有 encryptionConfig，或者 encryptionConfig 資源不包含密碼，則表示規則為「NON_COMPLIANT」。
- 如果用於加密 EKS 密碼的金鑰與參數不相符，則表示規則也是「NON_COMPLIANT」。

識別符：EKS_SECRETS_ENCRYPTED

資源類型： AWS::EKS::Cluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：CSV

EKS 叢集中應用來加密密碼的 KMS 金鑰 Amazon Resource Name (ARN) 清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-auto-minor-version-upgrade-check

檢查適用 ElastiCache 於 Redis 叢集的 Amazon 是否已啟用次要版本 auto 升級。如果 ElastiCache 叢集使用 Redis 引擎且 " 未設定為 'true'，則該規則對於叢集而言是 AutoMinor VersionUpgrade「不相容」。

識別符：ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

資源類型： AWS::ElastiCache::CacheCluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-rbac-auth-enabled

檢查 Amazon ElastiCache 複寫群組是否已啟用 RBAC 身份驗證。如果 Redis 版本為 6 或更高版本且「UserGroupIds」遺失、空白或不符合 " 參數提供的項目，則規則為「不相容」。`allowedUserGroupIDs`

識別符：ELASTICACHE_RBAC_AUTH_ENABLED

資源類型： AWS::ElastiCache::ReplicationGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

允許的 UserGroup ID (選擇性), 類型：CSV

已核准用於 ElastiCache 複寫群組存取的使用者群組識別碼清單 (逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-redis-cluster-automatic-backup-check

檢查 Amazon ElastiCache Redis 叢集是否已開啟自動備份功能。如果 Redis 叢集小於參數，則該規則 SnapshotRetentionLimit 為「不相容」。 SnapshotRetentionPeriod 例如：如果參數為 15，則如果介於 0-15 之間，則規則 snapshotRetentionPeriod 不相容。

識別符：ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

資源類型: AWS::ElastiCache::CacheCluster AWS::ElastiCache::ReplicationGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

snapshotRetentionPeriod (選擇性), 類型：int, 預設：15

Redis 叢集的最短快照保留期間 (以天為單位)。預設為 15 天。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-repl-grp-auto-failover-enabled

檢查 Amazon ElastiCache Redis 複寫群組是否已啟用自動容錯移轉。如果 " 未設定為「啟用」，則 ElastiCache 複寫群組的規則為 AutomaticFailover「不相容」。

識別符：ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

資源類型： AWS::ElastiCache::ReplicationGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-repl-grp-encrypted-at-rest

檢查 Amazon ElastiCache 複寫群組是否已 encryption-at-rest 啟用。如果停用 'AtRestEncryptionEnabled' 或 KMS 金鑰 ARN 不符合核准的 KMS 參數，則此規則對於 ElastiCache 複寫群組是「不符合」標準。KeyArns

識別符：ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

資源類型： AWS::ElastiCache::ReplicationGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

核准的 KMS KeyIds (選擇性), 類型：CSV

已核准 ElastiCache 使用的 KMS 金鑰識別碼 (逗號分隔) 清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-repl-grp-encrypted-in-transit

檢查 Amazon ElastiCache 複寫群組是否已 encryption-in-transit 啟用。如果將「TransitEncryption已啟用」設定為「假」，則 ElastiCache 複寫群組的規則為「不符合 _ 規範」。

識別符：ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

資源類型： AWS::ElastiCache::ReplicationGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-repl-grp-redis-auth-enabled

檢查 Amazon ElastiCache 複寫群組是否已啟用 Redis AUTH。如果 ElastiCache 複寫群組的節點版本低於 6 (第 6 版以上使用 Redis ACL) 且 " 遺失或為空白/空白，則此規則對於複寫群組而言是「不相容 AuthToken」。

識別符：ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

資源類型： AWS::ElastiCache::ReplicationGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-subnet-group-check

檢查 Amazon ElastiCache 叢集是否使用自訂子網路群組進行設定。如果叢集使用預設子網路 ElastiCache 群組，則該規則為「不符合」規則。

識別符：ELASTICACHE_SUBNET_GROUP_CHECK

資源類型： AWS::ElastiCache::CacheCluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticache-supported-engine-version

檢查 ElastiCache 叢集執行的版本是否大於或等於建議的引擎版本。如果 ElastiCache 叢集的 'EngineVersion' 小於其指定引擎的指定建議版本，則該規則為 NON_COMPLUTION。

識別符：ELASTICACHE_SUPPORTED_ENGINE_VERSION

資源類型： AWS::ElastiCache::CacheCluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最新 MemcachedVersion, 類型：字串

適用於 Memcached 的最新建議引擎版本。有效值採用語意版本化 (SemVer) 格式，主要版本、次要版本和修補程式版本的 3 個組件編號 (例如 1.6.6，而非 1.6)。

最新 RedisVersion, 類型：字串

適用於 Redis 的最新建議引擎版本。有效值採用語意版本化 (SemVer) 格式，主要版本、次要版本和修補程式版本的三個組件編號 (例如 7.0.5，而非 7.0)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticsearch-encrypted-at-rest

檢查 Amazon OpenSearch 服務 (先前稱為彈性搜尋) 網域是否已啟用靜態加密組態。如果未啟用此 EncryptionAtRestOptions 欄位，則規則為「不符合 _ 規範」。

識別符： ELASTICSEARCH_ENCRYPTED_AT_REST

資源類型： AWS::Elasticsearch::Domain

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticsearch-in-vpc-only

檢查 Amazon OpenSearch 服務（以前稱為彈性搜索）域是否位於 Amazon Virtual Private Cloud（Amazon VPC）中。如果 OpenSearch 服務網域端點是公用的，則該規則為「非 _ 相容」。

識別符： ELASTICSEARCH_IN_VPC_ONLY

資源類型： AWS::Elasticsearch::Domain

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticsearch-logs-to-cloudwatch

檢查 Amazon OpenSearch 服務網域是否設定為將日誌傳送到 Amazon CloudWatch 日誌。如果 Amazon ES 網域已啟用日誌，則表示規則為「COMPLIANT」。如果未設定日誌記錄，則表示規則為「NON_COMPLIANT」。

識別符：ELASTICSEARCH_LOGS_TO_CLOUDWATCH

資源類型： AWS::Elasticsearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

logTypes (選用), 類型：CSV

以逗號分隔的已啟用日誌清單。有效值為 'search'、'index'、'error'。

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*具有下列一或多個金鑰的物件：SEARCH_SLOW_LOGS、ES_APPLICATION_LOGS、INDEX_SLOW_LOGS、AUDIT_LOGS，取決於您想發佈的日誌類型。每個鍵都需要一個有效的 LogPublishingOption 值。

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elasticsearch-node-to-node-encryption-check

檢查 OpenSearch 服務（以前稱為 Elasticsearch）節點是否經過端對端加密。如果未在網域上啟用 node-to-node 加密，則該規則為「不符合 N_COMPLUTION」。

識別符：ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

資源類型： AWS::Elasticsearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COMPANTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
```

```
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elastic-beanstalk-logs-to-cloudwatch

檢查 E AWS lastic Beanstalk 環境是否設定為將日誌傳送到 Amazon CloudWatch 日誌。如果 `的值為假，則該規則為「不符合 _StreamLogs」。

識別符：ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

資源類型： AWS::ElasticBeanstalk::Environment

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

RetentionInDays (選擇性), 類型：字串

在保留日誌事件過期之前的天數。有效值為：1、3、5、7、14、30、60、90、120、150、180、365、400、545、731、1827 和 3653。該規則是不兼容的，如果 `日誌的值。 RetentionIn天數與此參數不符。

DeleteOnTerminate (選擇性), 類型：字串

檢查日誌是否設定為在終止環境時刪除。有效值為 `true` 或 `false`。該規則是不兼容的，如果 `日誌的值。 DeleteOn終止 `與此參數不匹配。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elastic-beanstalk-managed-updates-enabled

檢查 AWS Elastic Beanstalk 環境中的受管理平台更新是否已啟用。如果 `ManagedActionsEnabled` 的值設定為 true，則表示規則為「COMPLIANT」。如果 `ManagedActionsEnabled` 的值設定為 false，或者提供了參數且其值與現有組態不相符，則表示規則為「NON_COMPLIANT」。

識別符：ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

資源類型： AWS::ElasticBeanstalk::Environment

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

UpdateLevel (選擇性), 類型：字串

表示更新層級是設定為「次要」版本更新還是「修補程式」版本更新。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elbv2-acm-certificate-required

檢查應用程式負載平衡器和網路負載平衡器是否有設定為使用來自 AWS Certificate Manager (ACM) 憑證的接聽程式。如果至少 1 個負載平衡器至少有 1 個接聽程式，且該監聽器設定為不含來自 ACM 的憑證，或設定為使用與 ACM 憑證不同的憑證，則表示規則為「NON_COMPLIANT」。

識別符：ELBV2_ACM_CERTIFICATE_REQUIRED

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

AcmCertificatesAllowed (選擇性), 類型：CSV

以逗號分隔的憑證 Amazon Resource Name (ARN) 清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elbv2-multiple-az

檢查 Elastic Load Balancer V2 (應用程式、網路或閘道 Load Balancer) 是否對應至多個可用區域 (AZ)。如果 Elastic Load Balancer V2 對應至的 AZ 少於 2 個，則表示規則為「NON_COMPLIANT」。如需詳細資訊，請參閱《Application Load Balancer 的可用區域》。

識別符：ELBV2_MULTIPLE_AZ

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

minAvailabilityZones (選擇性), 類型：int

預期 AZ 的最小數量 (2 到 10 之間，包括 2 和 10)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elb-acm-certificate-required

檢查傳統負載平衡器是否使用由 AWS Certificate Manager提供的 SSL 憑證。若要使用此規則，請搭配使用 Classic Load Balancer 與 SSL 或 HTTPS 接聽程式。這個規則僅適用於 Classic Load Balancer。此規則不會檢查 Application Load Balancer 和網路負載平衡器。

識別符： ELB_ACM_CERTIFICATE_REQUIRED

資源類型： AWS::ElasticLoadBalancing::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elb-cross-zone-load-balancing-enabled

檢查是否啟用 Classic Load Balancer 的跨區域負載平衡。如果 Classic Load Balancer 未啟用跨區域負載平衡，則表示規則為「NON_COMPLIANT」。

識別符：ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

資源類型： AWS::ElasticLoadBalancing::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elb-custom-security-policy-ssl-check

檢查您的 Classic Load Balancer SSL 接聽程式是否使用自訂政策。規則僅適用於存在 Classic Load Balancer 的 SSL 接聽程式時。

識別符： ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

資源類型： AWS::ElasticLoadBalancing::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

SSL ProtocolsAnd 密碼, 類型：字串

以逗號分隔的密碼和通訊協定清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elb-deletion-protection-enabled

檢查 Elastic Load Balancer 是否已啟用刪除保護。如果 deletion_protection.enabled 為 false，則表示規則為「NON_COMPLIANT」。

識別符： ELB_DELETION_PROTECTION_ENABLED

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elb-logging-enabled

檢查 Application Load Balancer 和 Classic Load Balancer 是否已啟用日誌記錄。如果為假或`access_logs.S3.bucket`不等於您提供的 `access_logs.s3.enabled` s3，則BucketName 該規則為「不符合」。

> **Note**
>
> 此規則不適用於 Network Load Balancer 或 Gateway Load Balancer。

識別符： ELB_LOGGING_ENABLED

資源類型: AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

s3 BucketNames (選擇性的), 類型：CSV

傳送日誌檔案的 Amazon ELB 中 Amazon S3 儲存貯體名稱的清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elb-predefined-security-policy-ssl-check

檢查 Classic Load Balancer SSL 接聽程式是否使用預先定義的政策。如果 Classic Load Balancer HTTPS/SSL 接聽程式的政策不等於參數 '`predefinedPolicyName`' 的值，則表示規則為「NON_COMPLIANT」。

識別符： ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

資源類型： AWS::ElasticLoadBalancing::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

預定義 PolicyName, 類型：字串

預先定義的政策名稱。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## elb-tls-https-listeners-only

檢查您的 Classic Load Balancer 是設定使用 SSL 還是 HTTPS 接聽程式。如果接聽程式未設定使用 SSL 或 HTTPS ，則表示規則為「NON_COMPLIANT」。

- 如果 Classic Load Balancer 未設定接聽程式，則規則會傳回「NOT_APPLICABLE」。
- 如果 Classic Load Balancer 接聽程式設定使用 SSL 或 HTTPS ，則表示規則為「COMPLIANT」。
- 如果接聽程式未設定使用 SSL 或 HTTPS ，則表示規則為「NON_COMPLIANT」。

識別符：ELB_TLS_HTTPS_LISTENERS_ONLY

資源類型： AWS::ElasticLoadBalancing::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## emr-block-public-access

檢查 Amazon EMR 的帳戶是否已啟用封鎖公用存取設定。如果為 False，或者如果 BlockPublicSecurityGroupRules 為 true，則在中列出了通訊埠 22 以外的通訊埠，則規則為「不符合」。 PermittedPublicSecurityGroupRuleRanges

識別符：EMR_BLOCK_PUBLIC_ACCESS

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## emr-kerberos-enabled

檢查 Amazon EMR 叢集是否已啟用 Kerberos。如果安全組態未連接到叢集，或安全組態未滿足指定的規則參數，則表示規則為「NON_COMPLIANT」。

識別符： EMR_KERBEROS_ENABLED

資源類型： AWS::EMR::Cluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

TicketLifetimeInHours (選擇性), 類型：int

叢集 KDC 發行之 Kerberos 票證有效的期間。

Realm (選用), 類型：字串

在信任關係中另一個領域的 Kerberos 領域名稱。

Domain (選用), 類型：字串

信任關係中另一個領域的網域名稱。

AdminServer (選擇性), 類型：字串

在信任關係另一個領域中管理伺服器的完整網域。

KdcServer (選擇性), 類型：字串

在信任關係另一個領域中 KDC 伺服器的完整網域。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## emr-master-no-public-ip

檢查 Amazon EMR 叢集的主節點是否具有公有 IP。如果主節點具有公有 IP，則規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則會檢查處於 RUNNING 或 WAITING 狀態的叢集。此規則需要您啟用 `AWS::EC2::Instance` 資源類型的記錄，才能獲得準確的評估。

識別符：EMR_MASTER_NO_PUBLIC_IP

資源類型: AWS::EMR::Cluster, AWS::EC2::Instance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## encrypted-volumes

檢查連接的 Amazon EBS 磁碟區是否已加密，以及選擇性地使用指定的 KMS 金鑰加密。如果連接的 EBS 磁碟區未加密，或使用不在所提供參數中的 KMS 金鑰加密，則表示規則為「NON_COMPLIANT」。

識別符： ENCRYPTED_VOLUMES

資源類型： AWS::EC2::Volume

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

kmsId (Optional), 類型：字串

用於加密磁碟區的 KMS 金鑰的 ID 或 ARN。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fms-shield-resource-policy-check

檢查 Application Load Balancer、Amazon CloudFront 分發、Elastic Load Balancer 或彈性 IP 是否具有 AWS Shield 保護。它還會檢查它們是否具有與 Application Load Balancer 和 Amazon CloudFront 分發相關聯的 Web ACL。

識別符： FMS_SHIELD_RESOURCE_POLICY_CHECK

資源類型：平 AWS::CloudFront::Distribution, AWS::ElasticLoad衡 V2： ：LoadBalancer， AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoad平衡： ，LoadBalancer AWS::ShieldRegional::Protection AWS::Shield::Protection

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

webACLId, 類型：字串

Web ACL 的 WebACLId。

resourceTypes, 類型：字串

將套用此 config 規則的資源範圍。

resourceTags (選用), 類型：字串

規則應與其建立關聯的資源標籤 (例如 { "tagKey1" : ["tagValue1"]、"tagKey2" : ["tagValue2", "tagValue3"] })。

excludeResourceTags (選擇性), 類型：布林值

若為 true，則排除符合 resourceTags 的資源。若為 false，包含所有符合 resourceTags 的資源。

fmsManagedToken (選擇性), 類型：字串

AWS Firewall Manager 員在您的帳戶中建立規則時產生的權杖。 AWS Config 會在您建立此規則時忽略此參數。

fmsRemediationEnabled (選擇性), 類型：布林值

如果為 true，則 AWS Firewall Manager 員將根據 FMS 策略更新符合 NON_COMPF 的資源。 AWS Config 會在您建立此規則時忽略此參數。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fms-webacl-resource-policy-check

檢查 Web ACL 是否與 Application Load Balancer、API Gateway 階段或 Amazon CloudFront 分發相關聯。 AWS Firewall Manager 建立此規則時，FMS 原則擁有者會在 FMS 原則`WebACLId`中指定，並可選擇性地啟用修復。

識別符： FMS_WEBACL_RESOURCE_POLICY_CHECK

資源類型: AWS::CloudFront::Distribution, AWS::ApiGateway:: 階段 AWS::ElasticLoadBalancingV2::LoadBalancer, ACL AWS::WAFRegional::Web

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

webACLId, 類型：字串

Web ACL 的 WebACLId。

resourceTags (選用), 類型：字串

應與規則相關聯的資源標籤 (ApplicationLoad平衡器 ApiGatewayStage 和 CloudFront 分佈)。 （例如，{「標籤 1」：[「標籤值 1」]，「標籤鍵 2」：[「標籤值 2」，「標籤值 3」]}）

excludeResourceTags (選擇性), 類型：布林值

若為 true，則排除符合 resourceTags 的資源。

fmsManagedToken (選擇性), 類型：字串

AWS Firewall Manager 員在客戶帳戶中建立規則時產生的權杖。 AWS Config 會在客戶建立此規則時忽略此參數。

fmsRemediationEnabled (選擇性), 類型：布林值

如果為 true，則 AWS Firewall Manager 員將根據 FMS 策略更新不相容的資源。 AWS Config 會在客戶建立此規則時忽略此參數。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fms-webacl-rulegroup-association-check

檢查與 Web ACL 相關聯的規則群組優先順序是否正確。正確的優先順序是由 ruleGroups 參數中的規則群組排名所決定。 AWS Firewall Manager 建立此規則時，會指定最高優先順序 0，後跟 1、2 等。FMS 政策擁有者會指定 FMS 政策中的 `ruleGroups` 排名並可選擇啟用修補。

識別符： FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

資源類型: AWS::WAF::Web前十字韌帶, AWS::WAFRegional::Web ACL

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

ruleGroups, 類型：字串

以逗號分隔的 RuleGroupIds 和 WafOverrideAction 配對清單。（例如， ruleGroupId-1：無，2：計數） ruleGroupId

fmsManagedToken (選擇性), 類型：字串

AWS Firewall Manager 員在客戶帳戶中建立規則時產生的權杖。 AWS Config 會在客戶建立此規則時忽略此參數。

fmsRemediationEnabled (選擇性), 類型：布林值

如果為 true，則 AWS Firewall Manager 員將根據 FMS 策略更新不相容的資源。 AWS Config 會在客戶建立此規則時忽略此參數。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fsx-last-backup-recovery-point-created

檢查是否已為 Amazon FSx 檔案系統建立復原點。如果 Amazon FSx 檔案系統沒有在指定期間內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::FSx::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon FSx 檔案系統標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon FSx 檔案系統 ID。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fsx-lustre-copy-tags-to-backups

檢查 Amazon FSx for Lustre 檔案系統是否已設定為將標籤複製到備份。如果 Lustre 檔案系統未設定為將標籤複製到備份，則表示規則為「NON_COMPLIANT」。

識別符：FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

資源類型： AWS::FSx::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fsx-meets-restore-time-target

確認 Amazon FSx 檔案系統的還原時間是否符合指定的持續時間。如果 Amazon FSx 檔案系統 LatestRestoreExecutionTimeMinutes 的時間大於分鐘，則該規則為「不相容」。 maxRestoreTime

識別碼：FSX_MEETS_RESTORE_TIME_TARGET

資源類型： AWS::FSx::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 Amazon FSx 檔案系統標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon FSx 檔案系統 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fsx-openzfs-copy-tags-enabled

檢查 Amazon FSx for OpenZFS 檔案系統是否設定為將標籤複製到備份和磁碟區。如果 FSx for OpenZFS 檔案系統未設定為將標籤複製到備份和磁碟區，則表示規則為「NON_COMPLIANT」。

識別符：FSX_OPENZFS_COPY_TAGS_ENABLED

資源類型： AWS::FSx::FileSystem

觸發類型：定期

AWS 區域：只可在 歐洲 (斯德哥爾摩)、亞太區域 (孟買)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、亞太區域 (香港)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部) 區域使用

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fsx-resources-protected-by-backup-plan

檢查 Amazon FSx 檔案系統是否受備份計畫保護。如果備份計畫未涵蓋 Amazon FSx 檔案系統，則表示規則為「NON_COMPLIANT」。

識別符：FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::FSx::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon FSx 檔案系統標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 Amazon FSx 檔案系統 ID。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## fsx-windows-audit-log-configured

檢查 Amazon FSx for Windows File Server 檔案系統是否啟用了檔案存取稽核。如果 FSx for Windows File Server 檔案系統未啟用檔案存取稽核，則表示規則為「NON_COMPLIANT」。

識別符：FSX_WINDOWS_AUDIT_LOG_CONFIGURED

資源類型： AWS::FSx::FileSystem

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## global-endpoint-event-replication-enabled

檢查 Amazon EventBridge 全球端點是否已啟用事件複寫。如果未啟用事件複寫，則表示規則為「NON_COMPLIANT」。

識別符：GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

資源類型： AWS::Events::Endpoint

觸發類型： Configuration changes (組態變更)

AWS 區域: 僅在歐洲 (斯德哥爾摩)、亞太區域 (孟買)、歐洲 (巴黎)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (首爾)、亞太區域 (大阪)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (奧勒岡)、美國西部 (加利福尼亞)、亞太區域 (大阪)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利福尼亞) 雪梨), 加拿大 (中部) 區域

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 警衛-EK-保護審計啟用

檢查您帳戶中的 Amazon GuardDuty 偵測器是否已啟用亞馬遜彈性 Kubernetes 服務 (Amazon EKS) 的稽核日誌監控。如果您的帳戶未啟用 EKS 稽核記錄監視功能，則該規則為「不符合 _ 規範」。

識別碼：保護 EK_ 保護 _ 稽核 _ 啟用

資源類型： AWS::GuardDuty::Detector

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 防護-EK 保護-運行時啟用

檢查帳戶中的 GuardDuty 偵測器是否已啟用具有自動化代理程式管理的 Amazon EKS 執行階段監控。如果您的帳戶未啟用具有自動化代理程式管理的 EKS 執行階段監視，則 GuardDuty 此規則為「不符合 N_COMPON_COMP

識別碼：保護 EK_ 保護 _ 執行階段 _ 已啟用

資源類型： AWS::GuardDuty::Detector

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## guardduty-enabled-centralized

檢查您的 AWS 帳戶和 AWS 區域 GuardDuty 是否已啟用 Amazon。如果您提供集中化 AWS 帳戶，則規則會評估集中式帳戶中的 GuardDuty 結果。啟用時，規則 GuardDuty 為「相容」。

識別符： GUARDDUTY_ENABLED_CENTRALIZED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

CentralMonitoringAccount (選擇性), 類型：字串

允許集中 Amazon GuardDuty 結果的 AWS 帳戶（12 位數）的逗號分隔列表。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 啟用了防守羔羊保護

檢查您帳戶中的 Amazon GuardDuty 偵測器是否已啟用 Lambda 保護。如果您的帳戶未啟用 Amazon GuardDuty 中的 Lambda 保護功能，則該規則為「不符合 _ 規範」。

識別碼：已啟用保護

資源類型： AWS::GuardDuty::Detector

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 啟用安全防護惡意軟體保護

檢查您帳戶中的 Amazon GuardDuty 偵測器是否已啟用惡意軟體防護。如果您的帳戶未啟用 Amazon GuardDuty 中的惡意軟體防護功能，則該規則為「不符合」規則。

識別碼：保護 _ 惡意軟體 _ 保護 _ 啟用

資源類型： AWS::GuardDuty::Detector

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## guardduty-non-archived-findings

檢查 Amazon 是否 GuardDuty 有未存檔的發現項目。如果 GuardDuty 未封存的低/中/高嚴重性發現項目早於 /days/參數中指定的數字，則規則為 NON_COMPLIGENCE。 daysLowSev MediumSev `daysHighSev`

識別符：GUARDDUTY_NON_ARCHIVED_FINDINGS

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

daysLowSev (選擇性), 類型：int, 預設：30

允許 Amazon GuardDuty 低嚴重性發現項目保持非封存的天數。預設值是 30 天。

daysMediumSev (選擇性), 類型：int, 預設：7

允許 Amazon GuardDuty 中等嚴重程度發現項目保持非封存的天數。預設值是 7 天。

daysHighSev (選擇性), 類型：int, 預設：1

允許 Amazon GuardDuty 高嚴重性發現項目保持非封存的天數。預設值是 1 天。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 啟用防護-rds 保護

檢查您帳戶中的 Amazon GuardDuty 偵測器是否已啟用 Amazon 關聯式資料庫服務 (Amazon RDS) 保護。如果您的帳戶未啟用 Amazon 中的 Amazon RDS 保護功能，則該規則為「不合規」。 GuardDuty

識別碼：保護 _RDS_ 保護 _ 已啟用

資源類型： AWS::GuardDuty::Detector

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 安全防護-s3 保護啟用

檢查您帳戶中的 Amazon GuardDuty 偵測器是否已啟用 S3 保護。如果您的帳戶未啟用 Amazon GuardDuty 中的 S3 保護功能，則該規則為「不合規」。

識別碼：保護 _S3_ 保護 _ 已啟用

資源類型： AWS::GuardDuty::Detector

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-customer-policy-blocked-kms-actions

檢查您建立的受管 AWS Identity and Access Management (IAM) 政策是否不允許對 AWS KMS 金鑰進行封鎖的動作。如果受管 IAM 政策允許在 AWS KMS 金鑰上執行任何封鎖的動作，則該規則為「不符合 NON_ 規範」。

> **Note**
>
> 此規則不會評估 IAM 政策中的變數或條件。如需詳細資訊，請參閱 IAM 政策元素：變數和 IAM JSON 政策元素：IAM 使用者指南中的條件。

識別符：IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

資源類型： AWS::IAM::Policy

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

封鎖 ActionsPatterns, 類型：CSV

列出以逗號分隔的封鎖 KMS 動作模式清單。例如，您可以將 KMS: 解密 * 或公里:列為封鎖的動ReEncrypt 作模式。如果受管 IAM 政策允許此參數中列出的任何動作模式，則該規則為 NON_COMPLIANT。

排除PermissionBoundaryPolicy （可選），類型：布林值

布林值標記，用於排除用作許可界限的 IAM 政策評估。如果設定為 'true'，則規則將不會在評估中包含許可界限。否則，當值設為 'false' 時，系統會評估範圍中的所有 IAM 政策。預設值為 'false'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 啟用 Iam 外部存取分析器

檢查您的帳戶是否在每個區域中啟用了用於外部存取的 IAM 存取分析器。如果區域中沒有用於外部存取的分析器，或者「status」屬性未設定為「ACTIVED」，則規則為「不符合 NON_COMPORT」。

識別碼：IAM_ 外部 _ 存取 _ 分析器啟用

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-group-has-users-check

檢查 IAM 群組是否擁有至少一個 IAM 使用者。

識別符： IAM_GROUP_HAS_USERS_CHECK

資源類型： AWS::IAM::Group

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-inline-policy-blocked-kms-actions

檢查附加到 IAM 使用者、角色和群組的內嵌政策是否不允許對所有 AWS KMS 金鑰進行封鎖的動作。如果內嵌政策中的所有 AWS KMS 金鑰都允許任何封鎖的動作，則該規則為「不符合 NON_COMPLUTION」

識別符：IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

資源類型: AWS::IAM::Group AWS::IAM::Role, AWS::IAM::User

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

封鎖 ActionsPatterns, 類型：CSV

以逗號分隔的封鎖 KMS 動作模式清單，例如公里:*、KMS: 解密、公里:*。ReEncrypt

排除RoleByManagementAccount （可選），類型：布林值

如果角色只能由組織管理帳戶擔任，請排除角色。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-no-inline-policy-check

檢查是否未使用內嵌政策功能。如果 AWS Identity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組具有任何內嵌政策，則該規則為「不符合 N__」標準。

識別符：IAM_NO_INLINE_POLICY_CHECK

資源類型: AWS::IAM::User, AWS::IAM::Role, AWS::IAM::Group

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-password-policy

檢查 AWS Identity and Access Management (IAM) 使用者的帳戶密碼政策是否符合參數中指定的要求。如果帳戶密碼政策不符合指定的要求，則表示規則為「NON_COMPLIANT」。

> **Important**
>
> 規則參數的 `true` 和 `false` 值區分大小寫。如果 `true` 沒有以小寫提供，其會被視為 `false`.

> **Note**
>
> 預設 IAM 密碼政策的評估結果

使用預設 IAM 密碼政策時，此規則會標記為「不符合」。
受管規則和全域 IAM 資源類型
2022 年 2 月之前登入的全球 IAM 資源類型
(`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

識別符： IAM_PASSWORD_POLICY

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

RequireUppercaseCharacters (選擇性), 類型：布林值, 預設：true

密碼至少必須包含一個大寫字元。

RequireLowercaseCharacters (選擇性), 類型：布林值, 預設：true

密碼至少必須包含一個小寫字元。

RequireSymbols (選擇性), 類型：布林值, 預設：true

密碼至少必須包含一個符號。

RequireNumbers (選擇性), 類型：布林值, 預設：true

密碼至少必須包含一個數字。

MinimumPasswordLength (選擇性), 類型：int, 預設：14

密碼長度下限。

PasswordReusePrevention (選擇性), 類型：int, 預設：24

允許重複使用的密碼次數。

MaxPasswordAge (選擇性), 類型：int, 預設：90

密碼過期前的天數。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-policy-blacklisted-check

如果輸入參數中的 Amazon 資源名稱 (ARN) 政策附加到 IAM 資源，則檢查每個 AWS 身分識別和存取管理 (IAM) 資源。如果政策 ARN 連接至 IAM 資源，則表示規則為「NON_COMPLIANT」。

識別符： IAM_POLICY_BLACKLISTED_CHECK

資源類型: AWS::IAM::User, AWS::IAM::Group, AWS::IAM::Role

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

policyArns, 類型：CSV, 默認值：ARN：aw:iam:: aw:政策/ AdministratorAccess

不應連接至任何 IAM 實體的 IAM 政策 ARN 清單 (以逗號分隔)。

exceptionList (選用), 類型：CSV

以逗號分隔的資源類型清單和資源名稱配對清單。例如 users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3]。

> **Note**
>
> 對於例外清單，請指定資源的名稱，而不是完整 ARN。無效：`arn:aws:iam::444455556666:role/Admin`。有效：`Admin`。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-policy-in-use

檢查 IAM 政策 ARN 是否連接至 IAM 使用者、具有一或多個 IAM 使用者的群組，或是具有一或多個信任實體的 IAM 角色。

> **Note**
>
> 受管規則和全域 IAM 資源類型
> 2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
> 如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
> 為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

識別符：IAM_POLICY_IN_USE

資源類型： AWS::IAM::Policy

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

policyARN, 類型：字串

要檢查的 IAM 政策 ARN。

policyUsageType (選擇性), 類型：字串

指定政策是否要連接至 IAM 使用者、群組或角色。有效值為 IAM_USER、IAM_GROUP、IAM_ROLE 或 ANY。預設值為 ANY。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-policy-no-statements-with-admin-access

檢查您建立的 AWS Identity and Access Management (IAM) 政策是否具有允許對所有資源的所有動作授與權限的 Allow 陳述式。如果任何自訂受管 IAM 政策陳述式在 "Resource": "*" 上包括搭配 "Action": "*" 的 "Effect": "Allow"，則表示規則為「NON_COMPLIANT」。

> **Note**
> 此規則僅評估客戶管理政策。此規則不會評估內嵌原則或 AWS 受管理的策略。如需不同之處的詳細資訊，請參閱《IAM 使用者指南》中的受管政策和內嵌政策。

下列政策為「NON_COMPLIANT」：

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

下列政策為「COMPLIANT」：

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
```

```
"Resource": "*"
}
```

識別符： IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

資源類型： AWS::IAM::Policy

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

排除PermissionBoundaryPolicy （可選），類型：布林值

布林值標記，用於排除用作許可界限的 IAM 政策評估。如果設定為 'true'，則規則將不會在評估中包含許可界限。否則，當值設為 'false' 時，系統會評估範圍中的所有 IAM 政策。預設值為 'false'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-policy-no-statements-with-full-access

檢查您建立的 AWS Identity and Access Management (IAM) 政策是否將許可授與個別 AWS 資源上的所有動作。如果任何客戶受管 IAM 政策允許至少一項服務的完整存取權，則該規則為「NON_COMPON_」。 AWS

內容：建議遵循最低權限原則，在授予 AWS 服務許可時限制 IAM 政策中允許的動作。此方法有助於確保您僅授與必要的權限，方法是指定所需的確切動作，避免對服務使用不受限制的萬用字元，例如。`ec2:*`

在某些情況下，您可能希望允許具有類似前置詞的多個動作，例如DescribeFlow日誌和DescribeAvailability區域。在這些情況下，您可以將字尾萬用字元新增至常用前置字元 (例如，`ec2:Describe*`)。分組相關動作有助於避免達到 IAM 政策大小限制。

如果您使用帶有尾碼萬用字元的前置動作 (例如，)，此規則將傳回COMPETITED。`ec2:Describe*`只有在您使用不受限制的萬用字元 (例如) 時，此規則才會傳回「NON_COMPLUTION」。`ec2:*`

> **Note**
>
> 此規則僅評估客戶管理政策。此規則不會評估內嵌原則或 AWS 受管理的策略。如需不同之處的詳細資訊，請參閱《IAM 使用者指南》中的受管政策和內嵌政策。

識別符：IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

資源類型： AWS::IAM::Policy

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

排除PermissionBoundaryPolicy （可選），類型：布林值

布林值標記，用於排除用作許可界限的 IAM 政策評估。如果設定為 'true'，則規則將不會在評估中包含許可界限。否則，當值設為 'false' 時，系統會評估範圍中的所有 IAM 政策。預設值為 'false'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-role-managed-policy-check

檢查受管政策清單中指定的所有受管政策是否附加至 AWS Identity and Access Management (IAM) 角色。如果受管政策沒有連接到 IAM 角色，則表示規則為 NON_COMPLIANT。

識別符： IAM_ROLE_MANAGED_POLICY_CHECK

資源類型： AWS::IAM::Role

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

管理 PolicyArns, 類型：CSV

以逗號分隔的 AWS 受管政策清單 Amazon 資源名稱 (ARN)。如需詳細資訊，請參閱《IAM 使用者指南》中的 Amazon Resource Name (ARN) 和AWS 受管政策。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-root-access-key-check

檢查根使用者存取金鑰是否可用。如果使用者存取金鑰不存在，則表示規則為「COMPLIANT」。若可用，則為「NON_COMPLIANT」。

> **Note**
>
> 受管規則和全域 IAM 資源類型
> 2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::Policy``AWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
> 如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
> 為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

識別符： IAM_ROOT_ACCESS_KEY_CHECK

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-服務器證書過期檢查

檢查存儲在 AWS IAM 中的 IAM SSL/TLS 服務器證書是否已過期。如果 IAM 伺服器憑證已過期，則該規則為「不相容」。

識別碼：IAM_ 伺服器 _ 憑證 _ 過期 _ 檢查

資源類型： AWS::IAM::ServerCertificate

觸發類型：定期

AWS 區域：僅在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-user-group-membership-check

檢查 IAM 使用者是否為至少一個 IAM 群組的成員。

識別符： IAM_USER_GROUP_MEMBERSHIP_CHECK

資源類型： AWS::IAM::User

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

groupNames (選用), 類型：字串

以逗號分隔之 IAM 群組的清單，其中的 IAM 使用者必須為成員。

> **Note**
>
> 這個規則不支援含逗號的群組名稱。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-user-mfa-enabled

檢查 AWS Identity and Access Management (IAM) 使用者是否已啟用多重要素驗證 (MFA)。如果至少一個 IAM 使用者未啟用 MFA，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 受管規則和全域 IAM 資源類型
> 2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
> 如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
> 為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

識別符： IAM_USER_MFA_ENABLED

資源類型： AWS::IAM::User

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-user-no-policies-check

檢查您的 AWS Identity and Access Management (IAM) 使用者是否沒有附加政策。IAM 使用者應從 IAM 群組或角色繼承許可。如果至少有一個 IAM 使用者連接了政策，則表示規則為「NON_COMPLIANT」。

識別符： IAM_USER_NO_POLICIES_CHECK

資源類型： AWS::IAM::User

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## iam-user-unused-credentials-check

檢查您的 AWS Identity and Access Management (IAM) 使用者是否擁有在您提供的指定天數內未使用的密碼或作用中存取金鑰。如果有最近未使用的非作用中帳號，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 重新評估時間表
>
> 在第一次評估的 4 小時內重新評估此規則，對結果沒有任何影響。

受管規則和全域 IAM 資源類型
2022 年 2 月之前登入的全球 IAM 資源類型
(`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄。
為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

識別符： IAM_USER_UNUSED_CREDENTIALS_CHECK

資源類型： AWS::IAM::User

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大CredentialUsage年齡, 類型：int, 預設：90

憑證無法使用的天數上限。預設值為 90 天。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## restricted-ssh

> **Important**
> 針對此規則，規則識別符 (INCOMING_SSH_DISABLED) 和規則名稱 (restricted-ssh) 不同。

檢查是否可以存取安全群組的傳入 SSH 流量。如果安全群組中的傳入 SSH 流量 IP 地址受限時 (0.0.0.0/0 或 ::/0 以外的 CIDR)，則表示規則為 COMPLIANT。若可用，則為「NON_COMPLIANT」。

識別符：INCOMING_SSH_DISABLED

資源類型： AWS::EC2::SecurityGroup

觸發類型： Configuration changes (組態變更) 和 Periodic (定期)。

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 檢查器-ec2-掃描啟用

檢查您的單一帳戶或多帳戶環境是否已啟用 Amazon Inspector V2 EC2 掃描，以偵測 EC2 執行個體上的潛在漏洞和網路連線問題。如果未啟動 EC2 掃描，則該規則為「不符合 _」。

識別碼：檢測器 _EC2_ 掃描啟用

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 檢查器 ECR-掃描啟用

檢查您的單一帳戶或多帳戶環境是否已啟動 Amazon Inspector V2 ECR 掃描，以偵測容器映像中潛在的軟體弱點。如果未啟動 ECR 掃描，則該規則為「不相容」。

識別碼：檢測器 _ 掃描啟用

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 檢查器羔羊代碼掃描啟用

檢查您的單一帳戶或多帳戶環境是否已啟動 Amazon Inspector V2 Lambda 程式碼掃描，以偵測潛在的程式碼弱點。如果未啟動 Lambda 程式碼掃描，則該規則為「不相容」。

識別碼：已啟用檢查程式碼

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：僅適用於歐洲 (斯德哥爾摩)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、美國東部 (維吉尼亞北部)、歐洲 (倫敦)、亞太區域 (東京)、美國西部 (奧勒岡)、亞太區域 (新加坡)、亞太區域 (雪梨)

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 檢查員-羔羊標準掃描啟用

檢查您的單一帳戶或多帳戶環境是否已啟動 Amazon Inspector V2 Lambda 標準掃描，以偵測潛在的軟體弱點。如果未啟動 Lambda 標準掃描，則該規則為「不符合 _」。

識別碼：檢查器標準 _ 掃描啟用

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ec2-instances-in-vpc

> **Important**
>
> 此規則的規則識別符 (INSTANCES_IN_VPC) 和規則名稱 (ec2-instances-in-vpc) 不同。

檢查您的 EC2 執行個體是否屬於虛擬私有雲端 (VPC)。您可選擇性指定與執行個體關聯的 VPC ID。

識別符： INSTANCES_IN_VPC

資源類型： AWS::EC2::Instance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

vpcId (選用), 類型：字串

包含這些 EC2 執行個體的 VPC ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## internet-gateway-authorized-vpc-only

檢查網際網路閘道是否連接至授權的虛擬私有雲端 (Amazon VPC)。如果網際網路閘道已連接至未經授權的 VPC，則表示規則為「NON_COMPLIANT」。

識別符： INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

資源類型： AWS::EC2::InternetGateway

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

AuthorizedVpcIds (選擇性), 類型：字串

包含連接 IGW 之授權 VPC ID 的逗號分隔清單。如果未提供參數，所有連接的 IGW 將為 NON_COMPLIANT。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 中國火花交付流加密

檢查 Amazon Kinesis Data Firehose 交付串流是否已使用伺服器端加密的靜態加密。如果 Kinesis Data Firehose 傳送串流在靜態時未使用伺服器端加密來加密，則該規則為「不相容」。

標識符：激光 _ 火警 _ 交付 _ 流加密

資源類型： AWS::KinesisFirehose::DeliveryStream

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：CSV

已核准用於 Kinesis Firehose 使用的 KMS 金鑰臂清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## kinesis-stream-encrypted

檢查 Amazon Kinesis 串流是否使用伺服器端加密進行靜態加密。如果 " 不存在，則該規則對於 Kinesis 串流是「不符合 _StreamEncryption」的規則。

內容：伺服器端加密是 Amazon Kinesis Data Streams 中的一項功能，可在資料處於靜態狀態之前使用 AWS KMS 金鑰自動加密。資料會在寫入 Kinesis 串流儲存層之前加密，並在從儲存體擷取資料後解密。因此，您的資料將於 Kinesis Data Streams 服務中靜態加密。這可幫助您符合法規要求，並增強資料的安全性。如需詳細資訊，請參閱《Amazon Kinesis Data Streams 中的資料保護》。

識別符：KINESIS_STREAM_ENCRYPTED

資源類型： AWS::Kinesis::Stream

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## kms-cmk-not-scheduled-for-deletion

檢查金 AWS 鑰管理服務 (AWS KMS) 金鑰是否未排定在 AWS KMS 中刪除。如果已排程刪除 KMS 金鑰，則該規則為「不符合 _」。

識別符： KMS_CMK_NOT_SCHEDULED_FOR_DELETION

資源類型： AWS::KMS::Key

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyIds (選擇性), 類型：字串

(選用) 未排定刪除之特定客戶受管金鑰 ID 的清單 (以逗號分隔)。如果未指定任何金鑰，則表示規則會檢查所有金鑰。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## lambda-concurrency-check

檢查 Lambda 函數是否已設定函數層級的並行執行限制。如果 Lambda 函數未設定函數層級的並行執行限制，則表示規則為「NON_COMPLIANT」。

識別符： LAMBDA_CONCURRENCY_CHECK

資源類型： AWS::Lambda::Function

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

ConcurrencyLimitLow (選擇性), 類型：字串

最低並行執行限制

ConcurrencyLimitHigh (選擇性), 類型：字串

最高並行執行限制

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## lambda-dlq-check

檢查 Lambda 函數是否設定無效字母佇列。如果 Lambda 函數未設定無效字母佇列，則表示規則為「NON_COMPLIANT」。

識別符： LAMBDA_DLQ_CHECK

資源類型： AWS::Lambda::Function

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

dlqArns (選用), 類型：字串

以逗號分隔的 Amazon SQS 和 Amazon SNS ARN 清單，其必須設定為 Lambda 函數無效字母佇列目標。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## lambda-function-public-access-prohibited

檢查連接至 Lambda 資源的 AWS Lambda 函數政策是否禁止公開存取。如果 Lambda 函數政策允許公共存取，則表示其為「NON_COMPLIANT」。

上下文：如果主體元素為空或包含萬用字元，則 Lambda 函數政策被視為允許公用存取。例如，如果主元素是“”或{“AWS”: “”}。出於安全原因，不建議授予公共訪問權限。限制公開存取可協助您防止 Lambda 函數遭到未經授權的呼叫，進而危及您的資料或產生不必要的成本。

若要限制對 Lambda 函數的存取，請指定可叫用函數的 IAM 使用者、角色或服務的 AWS 帳戶 ID 或 Amazon 資源名稱 (ARN)。如需詳細資訊，請參閱AWS Lambda 開發人員指南中的授與其他帳戶的功能存取權。

識別符： LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

資源類型： AWS::Lambda::Function

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## lambda-function-settings-check

檢查執行階段、角色、逾時和記憶體大小的 AWS Lambda 函數設定是否符合預期值。此規則會忽略「Image」套件類型的函數，以及執行階段設定為「僅限作業系統執行階段」的函數。如果 Lambda 函數設定與預期值不相符，則表示規則為「NON_COMPLIANT」。

識別符： LAMBDA_FUNCTION_SETTINGS_CHECK

資源類型： AWS::Lambda::Function

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

runtime, 類型：CSV

AWS Lambda 執行階段值的逗號分隔清單

role (選用), 類型：字串

AWS Lambda 執行角色的名稱或 ARN

timeout (選用), 類型：int, 預設：3

AWS Lambda 函數逾時 (秒)

memorySize (選用), 類型：int, 預設：128

AWS 以兆字節為單位的 Lambda 函數大小

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。為了讓此規則在主動模式下傳回 COLUTION，StartResource評估 API 的資源組態結構描述必須包含下列輸入，編碼為字串：

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* 如需有關這些輸入有效值的詳細資訊 MemorySize，請參閱《使用指南》中的〈角色、執行階段和逾時 AWS CloudFormation 〉。

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## lambda-inside-vpc

檢查是否允許 Lambda 函數存取虛擬私有雲端 (VPC)。如果 Lambda 函數未啟用 VPC，則表示規則為「NON_COMPLIANT」。

識別符： LAMBDA_INSIDE_VPC

資源類型： AWS::Lambda::Function

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

subnetIds (選用), 類型：字串

Lambda 函數可與之關聯的子網路 ID 清單 (以逗號分隔)。

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## lambda-vpc-multi-az-check

檢查 Lambda 是否有超過 1 個相關聯的可用區域。如果只有 1 個可用區域與 Lambda 相關聯，或者相關聯的可用區域數量少於選用參數中指定的數量，則表示規則為「NON_COMPLIANT」。

識別符：LAMBDA_VPC_MULTI_AZ_CHECK

資源類型： AWS::Lambda::Function

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

availabilityZones (選用), 類型：int

預期的可用區域數量。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## Macie-自動敏感的數據發現檢查

檢查 Amazon Macie 是否已啟用自動化敏感資料探索功能。如果停用自動化敏感資料探索，則該規則為「NON_COLUTION」。該規則適用於管理員帳戶，不適用於成員帳戶。

識別碼：MACIE_ 自動感應資料探索 _ 檢查

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## macie-status-check

檢查您的帳戶是否在每個區域中啟用 Amazon Macie。如果 'status' 屬性未設定為 'ENABLED'，則表示規則為「NON_COMPLIANT」。

識別符：MACIE_STATUS_CHECK

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mfa-enabled-for-iam-console-access

檢查使用主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者是否已啟用 AWS 多因素驗證 (MFA)。啟用 MFA 時，則表示規則為「COMPLIANT」。

> **Note**
>
> 重新評估時間表
> 在第一次評估的 4 小時內重新評估此規則，對結果沒有任何影響。
> 受管規則和全域 IAM 資源類型
> 2022 年 2 月之前登入的全球 IAM 資源類型
> (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法

在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

Identifier: (識別符：) MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

資源類型： AWS::IAM::User

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mq-active-deployment-mode

檢查針對 Amazon MQ ActiveMQ 代理程式引擎設定的部署模式。如果使用預設的單一執行個體代理程式模式，則表示規則為「NON_COMPLIANT」。

識別符：MQ_ACTIVE_DEPLOYMENT_MODE

資源類型： AWS::AmazonMQ::Broker

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mq-automatic-minor-version-upgrade-enabled

檢查是否已為 Amazon MQ 代理程式啟用自動次要版本升級。如果 Amazon MQ 代理程式未啟用 'AutoMinorVersionUpgrade' 欄位，則該規則為「不相容」。

識別符：MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

資源類型： AWS::AmazonMQ::Broker

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mq-auto-minor-version-upgrade-enabled

檢查是否已為 Amazon MQ 代理程式啟用自動次要版本升級。如果 Amazon MQ 代理程式未啟用 'AutoMinorVersionUpgrade' 欄位，則該規則為「不相容」。

識別符：MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

資源類型： AWS::AmazonMQ::Broker

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mq-cloudwatch-audit-logging-enabled

檢查 Amazon MQ 代理程式是否已啟用 Amazon CloudWatch 稽核記錄功能。如果代理程式未啟用稽核記錄，則表示規則為「NON_COMPLIANT」。

識別符：MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

資源類型： AWS::AmazonMQ::Broker

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mq-雲觀察審計日誌啟用

檢查 Amazon MQ 代理程式是否已啟用 CloudWatch 稽核記錄。如果代理程式未啟用稽核記錄，則該規則為「NON_ 相容」。

識別碼：啟用 MQ_ 雲監察 _ 稽核記錄

資源類型： AWS::AmazonMQ::Broker

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mq-no-public-access

檢查 Amazon MQ 代理程式是否無法公開存取。如果 Amazon MQ 代理程式的 'PubliclyAccessible' 欄位設定為 true，則該規則為「不相容」。

識別符：MQ_NO_PUBLIC_ACCESS

資源類型： AWS::AmazonMQ::Broker

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## mq-rabbit-deployment-mode

檢查針對 Amazon MQ RabbitMQ 代理程式引擎設定的部署模式。如果使用預設的單一執行個體代理程式模式，則表示規則為「NON_COMPLIANT」。

識別符：MQ_RABBIT_DEPLOYMENT_MODE

資源類型： AWS::AmazonMQ::Broker

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## msk-enhanced-monitoring-enabled

檢查是否已針對設定為 PER_TOPIC_PER_BROKER 或 PER_TOPIC_PER_PARTITION 的 Amazon MSK 叢集啟用增強型監控功能。如果已啟用增強型監控功能並設定為 DEFAULT 或 PER_BROKER，則表示規則為「NON_COMPLIANT」。

識別符：MSK_ENHANCED_MONITORING_ENABLED

資源類型： AWS::MSK::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## msk-in-cluster-node-require-tls

檢查 Amazon MSK 叢集是否使用 HTTPS (TLS) 對叢集的代理程式節點強制執行傳輸中加密。如果叢集內代理程式節點連線已啟用純文字通訊，則表示規則為「NON_COMPLIANT」。

識別符：MSK_IN_CLUSTER_NODE_REQUIRE_TLS

資源類型： AWS::MSK::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## Amazon CloudWatch Logs

> **Important**
>
> 針對此規則，規則識別符 (MULTI_REGION_CLOUD_TRAIL_ENABLED) 和規則名稱 (multi-region-cloudtrail-enabled) 不同。

檢查是否至少有一個多區域 AWS CloudTrail。如果追蹤不符合輸入參數，則表示規則為「NON_COMPLIANT」。如果`ExcludeManagementEventSources`欄位不為空或設定為排除管理事件 (例如 AWS CloudTrail 事件或 Amazon RDS 資料 API 事件)，則該規則為 AWS KMS 「非符合規範」。

Identifier: (識別符：) MULTI_REGION_CLOUD_TRAIL_ENABLED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

s3 BucketName (選擇性的), 類型：字串

將日誌檔交付 AWS CloudTrail 到的 Amazon S3 儲存貯體的名稱。

snsTopicArn (選擇性), 類型：字串

用於 AWS CloudTrail 通知的 Amazon SNS 主題 ARN。

雲端 WatchLogsLogGroupArn (選擇性), 類型：字串

Amazon CloudWatch 日誌組 ARN 用於 AWS CloudTrail 將數據發送到。

includeManagementEvents (選擇性), 類型：布林值

事件選取器，以包含的管理事件 AWS CloudTrail。

readWriteType (選擇性), 類型：字串

要記錄的事件類型。有效值為 ReadOnly， WriteOnly 且 ALL。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## nacl-no-unrestricted-ssh-rdp

檢查網路存取控制清單 (NACL) SSH/RDP 輸入流量的預設連接埠是否不受限制。如果 NACL 傳入項目允許連接埠 22 或 3389 使用來源 TCP 或 UDP CIDR 區塊，則表示規則為「NON_COMPLIANT」。

識別符：NACL_NO_UNRESTRICTED_SSH_RDP

資源類型： AWS::EC2::NetworkAcl

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-backup-retention-check

檢查 Amazon Neptune DB 叢集保留期間是否設定為特定天數。如果保留期間小於參數指定的值，則表示規則為「NON_COMPLIANT」。

識別符：NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

最小值 BackupRetentionPeriod (選擇性), 類型：int

備份最少應保留的天數。有效值為 1 到 35，預設值為 7。如果值大於「備份」，則規則為「不相容」RetentionPeriod。如果值小於或等於「備份RetentionPeriod」，則規則符合標準。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-cloudwatch-log-export-enabled

檢查 Amazon Neptune 叢集是否已 CloudWatch 為稽核日誌啟用日誌匯出功能。如果 Neptune 叢集沒有為稽核記錄啟用 CloudWatch 記錄匯出，則該規則為「NON_COMPLUTION」。

識別符：NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-copy-tags-to-snapshot-enabled

檢查 Amazon Neptune 叢集是否設定為在建立快照時將所有標籤複製到快照。如果「複製TagsTo快照」設定為 false，則該規則為「不符合 _」。

識別符：NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-deletion-protection-enabled

檢查 Amazon Neptune DB 叢集是否已啟用刪除保護。如果 Amazon Neptune 叢集的 deletionProtection 欄位設為 false，則表示規則為「NON_COMPLIANT」。

識別符：NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-encrypted

檢查您的 Amazon Neptune DB 叢集是否已啟用儲存加密。如果未啟用儲存加密，則表示規則為「NON_COMPLIANT」。

識別符：NEPTUNE_CLUSTER_ENCRYPTED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

KmsKeyArns (選擇性), 類型：CSV

要與加密叢集進行比較的 KMS 金鑰 ARN 清單 (逗號分隔)。 KmsKeyId

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-iam-database-authentication

檢查 Amazon Neptune 叢集是否已啟用 AWS Identity and Access Management (IAM) 資料庫身份驗證。如果 Amazon Neptune 叢集未啟用 IAM 資料庫身分驗證，則表示規則為「NON_COMPLIANT」。

識別符：NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-multi-az-enabled

檢查 Amazon Neptune 叢集是否已設定 Amazon RDS Multi-AZ 複寫。如果未啟用 Multi-AZ 複寫，則表示規則為「NON_COMPLIANT」。

識別符：NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-snapshot-encrypted

檢查 Amazon Neptune DB 叢集是否已為快照加密。如果 Neptune 叢集沒有為快照加密，則表示規則為「NON_COMPLIANT」。

識別符：NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

資源類型:AWS:: RDS:: 資料庫 ClusterSnapshot

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## neptune-cluster-snapshot-public-prohibited

檢查 Amazon Neptune 手動 DB 叢集快照是否為公有狀態。如果任何現有和新的 Neptune 叢集快照為公有狀態，則表示規則為「NON_COMPLIANT」。

識別符：NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

資源類型:AWS:: RDS:: 資料庫 ClusterSnapshot

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## netfw-deletion-protection-enabled

檢查 AWS Network Firewall 是否已啟用刪除保護。如果 Network Firewall 未啟用刪除保護，則表示規則為「NON_COMPLIANT」。

識別符：NETFW_DELETION_PROTECTION_ENABLED

資源類型： AWS::NetworkFirewall::Firewall

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## netfw-logging-enabled

檢查 AWS Network Firewall 防火牆是否已啟用記錄。如果未設定日誌記錄類型，則表示規則為「NON_COMPLIANT」。您可以指定要規則檢查的日誌記錄類型。

識別符：NETFW_LOGGING_ENABLED

資源類型： AWS::NetworkFirewall::LoggingConfiguration

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

logType (選用), 類型：字串

logType (選用)：要檢查防火牆之規則的日誌類型：'alert'、'flow' 或 'both'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## netfw-multi-az-enabled

檢查 AWS Network Firewall 防火牆是否跨多個可用區域部署。如果防火牆僅部署在一個可用區域中，或部署在少於選用參數中列出數量的區域中，則表示規則為「NON_COMPLIANT」。

識別符：NETFW_MULTI_AZ_ENABLED

資源類型： AWS::NetworkFirewall::Firewall

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

availabilityZones (選用), 類型：int

預期的可用區域數量。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## netfw-policy-default-action-fragment-packets

檢查 AWS Network Firewall 策略是否設定了使用者定義的零散封包的無狀態預設動作。如果分段封包無狀態預設動作與使用者定義的預設動作不相符，則表示規則為「NON_COMPLIANT」。

識別符：NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

資源類型： AWS::NetworkFirewall::FirewallPolicy

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無狀態FragmentDefault動作, 類型：CSV

> 以逗號分隔的值清單。您最多可以選擇兩項。有效值包含 'aws:pass'、'aws:drop' 和 'aws:forward_to_sfe'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## netfw-policy-default-action-full-packets

檢查 AWS Network Firewall 策略是否設定了使用者針對完整封包定義的預設無狀態動作。如果完整封包預設無狀態動作與使用者定義的預設無狀態動作不相符，則表示此規則為「NON_COMPLIANT」。

識別符：NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

資源類型： AWS::NetworkFirewall::FirewallPolicy

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無國籍 DefaultActions, 類型：CSV

以逗號分隔的值清單。您最多可以選擇兩項。有效值包含 'aws:pass'、'aws:drop' 和 'aws:forward_to_sfe'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## netfw-policy-rule-group-associated

檢查 AWS Network Firewall 策略是否與可設定狀態或無狀態規則群組相關聯。如果沒有具狀態或無狀態的規則群組與 Network Firewall 策略相關聯，則表示此規則為「NON_COMPLIANT」(如果其中一個規則群組存在)。

識別符：NETFW_POLICY_RULE_GROUP_ASSOCIATED

資源類型： AWS::NetworkFirewall::FirewallPolicy

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## netfw-stateless-rule-group-not-empty

檢查無狀態 Network Firewall 規則群組是否包含規則。如果無狀態 Network Firewall 規則群組中沒有規則，則表示規則為「NON_COMPLIANT」。

識別符：NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

資源類型： AWS::NetworkFirewall::RuleGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## nlb-cross-zone-load-balancing-enabled

檢查是否在 Network Load Balancer (NLB) 上啟用跨區域負載平衡。如果 NLB 未啟用跨區域負載平衡，則表示規則為「NON_COMPLIANT」。

識別符：NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

資源類型： AWS::ElasticLoadBalancingV2::LoadBalancer

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## no-unrestricted-route-to-igw

檢查路由表中是否有通往網際網路閘道 (IGW) 的公有路由。如果 IGW 的路由具有 '0.0.0.0/0' 或 '::/0' 的目的地 CIDR 區塊，或者目標 CIDR 區塊與規則參數不相符，則表示規則為「NON_COMPLIANT」。

識別符：NO_UNRESTRICTED_ROUTE_TO_IGW

資源類型： AWS::EC2::RouteTable

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

routeTableIds (選擇性), 類型：CSV

以逗號分隔的路由表格 ID 清單，這些路由表格 ID 可能有目的地 CIDR 區塊為 '0.0.0.0/0' 或 '::/0'.' 的網際網路閘道。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-access-control-enabled

檢查 Amazon OpenSearch 服務網域是否啟用了精細的存取控制。如 AdvancedSecurityOptions 果未針對 OpenSearch 服務網域啟用，則該規則為「不相容」。

識別符：OPENSEARCH_ACCESS_CONTROL_ENABLED

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-audit-logging-enabled

檢查 Amazon OpenSearch 服務網域是否已啟用稽核記錄。如果 OpenSearch 服務網域未啟用稽核記錄，則該規則為「非符合規範」。

識別符：OPENSEARCH_AUDIT_LOGGING_ENABLED

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

雲端 WatchLogsLogGroupArnList (選擇性), 類型：CSV

> Amazon CloudWatch 日誌記錄群組的 Amazon 資源名稱 (ARN) 清單 (逗號分隔)。此規則會檢查指定的記錄群組是否已針對稽核記錄設定。
>
> 有效值包括：`arn:aws:logs:region:account-id:log-group:log_group_name:*` 與 `arn:aws:logs:region:account-id:log-group:log_group_name`。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-data-node-fault-tolerance

檢查 Amazon OpenSearch 服務網域是否設定至少有三個資料節點且 zoneAwarenessEnabled 為真。如果「實例驗證」小於 3 或將「區 OpenSearch 域」設置為「假」，則該規則對於域來說是「AwarenessEnabled不符合 _」。

識別符：OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-encrypted-at-rest

檢查 Amazon OpenSearch 服務網域是否已啟用靜態加密組態。如果 `EncryptionAtRestOptions` 欄位為未啟用，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則不會評估 Elasticsearch 網域。

識別符：OPENSEARCH_ENCRYPTED_AT_REST

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-https-required

檢查 OpenSearch 網域的連線是否使用 HTTPS。如果 Amazon OpenSearch 網域「EnforceHTTPS」不是「真」或「真」且「TLS」不在 " 中，則該規則為「不符合SecurityPolicy」。`tlsPolicies`

識別符：OPENSEARCH_HTTPS_REQUIRED

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

tlsPolicies (選用), 類型：CSV

要對照 Amazon OpensSearch 網域進行檢查的 TLS 安全政策清單 (逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-in-vpc-only

檢查 Amazon OpenSearch 服務域是否位於 Amazon Virtual Private Cloud (VPC) 中。如果 OpenSearch 服務網域端點是公用的，則該規則為「非 _ 相容」。

> **Note**
>
> 此規則不會評估 Elasticsearch 網域。

識別符：OPENSEARCH_IN_VPC_ONLY

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-logs-to-cloudwatch

檢查 Amazon OpenSearch 服務網域是否設定為將日誌傳送到 Amazon CloudWatch 日誌。如果未啟用日誌，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則不會評估 Elasticsearch 網域。

識別符：OPENSEARCH_LOGS_TO_CLOUDWATCH

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

logTypes (選用), 類型：CSV

以逗號分隔的已啟用日誌清單。有效值為 'search'、'index'、'error'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-node-to-node-encryption-check

檢查 Amazon OpenSearch 服務節點是否經過端對端加密。如果未在網域上啟用 node-to-node 加密，則該規則為「不符合 N_COMPON_COMPORT

> **Note**
>
> 此規則不會評估 Elasticsearch 網域。

識別符：OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 打開搜索主要節點容錯

檢查 Amazon OpenSearch 服務網域是否設定至少有三個專用主節點。如果「DedicatedMaster已啟用」設定為「假」或「DedicatedMaster計數」小於 3，則該規則對於 OpenSearch 服務網域來說是「不符合 _ 規範」。

識別碼：開啟搜尋 _ 主要 _ 節點 _ 錯誤 _ 公差

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## opensearch-update-check

檢查 Amazon OpenSearch 服務版本更新是否可用，但未安裝。如果未安裝最新的軟體更新，則該規則適用於 OpenSearch 網域的「非符合規範」。

識別符：OPENSEARCH_UPDATE_CHECK

資源類型： AWS::OpenSearch::Domain

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-aurora-mysql-audit-logging-enabled

檢查 Amazon Aurora 與 MySQL 相容的版本叢集是否設定為將稽核日誌發佈到 Amazon 日誌。 CloudWatch 如果 Aurora MySQL 相容版本叢集未設定為發布稽核記錄，則規則為 NON_COMPLIANT。

識別符：RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-automatic-minor-version-upgrade-enabled

檢查 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體是否設定為進行自動次要版本升級。如果「auto MinorVersion 升級」的值為假，則規則為「不相容」。

識別符：RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COMPANTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

* 如需有關這些輸入有效值的詳細資訊，請參閱 AWS CloudFormation 使用指南中的〈引擎〉AutoMinorVersionUpgrade 和〈引擎〉。

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-cluster-auto-minor-version-upgrade-enable

檢查 Amazon RDS Multi-AZ 叢集部署是否已啟用自動次要版本升級。如果「 autoMinorVersion升級」設定為 false，則規則為「不符合 _」。

識別符：RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-cluster-default-admin-check

檢查 Amazon Relational Database Service (Amazon RDS) 資料庫叢集是否已變更預設值的管理員使用者名稱。如果管理員使用者名稱設定為預設值，則表示規則為「NON_COMPLIANT」。

識別符：RDS_CLUSTER_DEFAULT_ADMIN_CHECK

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

有效AdminUserNames （可選），類型：CSV

Amazon RDS 叢集可使用的管理員使用者名稱清單 (以逗號分隔)。因為 'postgres' 或 'admin' 為預設值，所以有效使用者名稱不能包含這兩個字串。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-cluster-deletion-protection-enabled

檢查 Amazon Relational Database Service (Amazon RDS) 叢集是否已啟用刪除保護。如果 Amazon RDS 叢集未啟用刪除保護，則表示規則為「NON_COMPLIANT」。

識別符：RDS_CLUSTER_DELETION_PROTECTION_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-cluster-encrypted-at-rest

檢查 Amazon Relational Database Service (Amazon RDS) 叢集是否經過靜態加密。如果 Amazon RDS 叢集未經過靜態加密，則表示規則為「NON_COMPLIANT」。

識別符：RDS_CLUSTER_ENCRYPTED_AT_REST

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-cluster-iam-authentication-enabled

檢查 Amazon Relational Database Service (Amazon RDS) 叢集是否已啟用 AWS Identity and Access Management (IAM) 身分驗證。如果 Amazon RDS 叢集未啟用 IAM 身分驗證，則表示規則為「NON_COMPLIANT」。

識別符： RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-cluster-multi-az-enabled

檢查 Amazon Relational Database Service (Amazon RDS) 管理的 Amazon Aurora 和 Hermes 叢集是否已啟用多可用區域 (異地同步備份) 複寫。如果 Amazon RDS 執行個體未使用異地同步備份設定，則表示規則為「NON_COMPLIANT」。

識別符：RDS_CLUSTER_MULTI_AZ_ENABLED

資源類型：AWS::RDS::DBCluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-db-security-group-not-allowed

檢查是否有任何不是預設 DB 安全群組的 Amazon Relational Database Service (Amazon RDS) DB 安全群組。如果有任何不是預設 DB 安全群組的 DB 安全群組，則表示規則為「NON_COMPLIANT」。

識別符：RDS_DB_SECURITY_GROUP_NOT_ALLOWED

資源類型:AWS:: RDS:: 資料庫 SecurityGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：僅適用於歐洲 (愛爾蘭)、南美洲 (聖保羅)、美國東部 (維吉尼亞北部)、亞太區域 (東京)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、亞太區域 (新加坡)、亞太區域 (雪梨) 區域

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-enhanced-monitoring-enabled

檢查 Amazon RDS 執行個體是否已啟用增強型監控功能。如果 RDS 執行個體之組態項目中的 `'monitoringInterval'` 為 '0'，或者 `'monitoringInterval'` 與規則參數值不相符，則表示此規則為「NON_COMPLIANT」。

識別符：RDS_ENHANCED_MONITORING_ENABLED

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

monitoringInterval (選用), 類型：int

為資料庫執行個體收集增強型監控指標之時間點之間的整數值，以秒為單位。有效值是 1、5、10、15、30 和 60。

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* 如需有關這些輸入有效值的詳細資訊，請參閱 AWS CloudFormation 使用指南中的〈引擎〉MonitoringInterval和〈引擎〉。

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-instance-default-admin-check

檢查 Amazon Relational Database Service (Amazon RDS) 資料庫是否已變更其預設值的管理員使用者名稱。此規則只會在 RDS 資料庫執行個體上執行。如果管理員使用者名稱設定為預設值，則表示規則為「NON_COMPLIANT」。

識別符：RDS_INSTANCE_DEFAULT_ADMIN_CHECK

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

有效AdminUserNames （ 可選 ）, 類型：CSV

Amazon RDS 執行個體可使用的管理員使用者名稱清單 (以逗號分隔)。(因為 'postgres' 或 'admin' 為預設值，所以有效使用者名稱不能包含這兩個字串。)

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-instance-deletion-protection-enabled

檢查 Amazon Relational Database Service (Amazon RDS) 執行個體是否已啟用刪除保護。如果 Amazon RDS 執行個體未啟用刪除保護，例如 deletionProtection 設定為 false，則表示規則為「NON_COMPLIANT」。

> **Warning**
> 叢集內的部分 RDS 資料庫執行個體 (Aurora/DocumentDB) 會顯示為不合規。

識別符：RDS_INSTANCE_DELETION_PROTECTION_ENABLED

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

databaseEngines (選用), 類型：CSV

要包含在規則評估中的 RDS 資料庫引擎清單 (以逗號分隔)。例如 'mysql, postgres, mariadb'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-instance-iam-authentication-enabled

檢查 Amazon Relational Database Service (Amazon RDS) 執行個體是否已啟用 AWS Identity and Access Management (IAM) 身分驗證。如果 Amazon RDS 執行個體未啟用 IAM 身分驗證，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 資料庫引擎應該是'mysql'、'postgres'、'aurora'、'aurora-mysql' 或 'aurora-postgresql' 中的其中一項。資料庫執行個體狀態應為 'available'、'backing-up'、'storage-optimization' 或 'storage-full' 中的其中一項。

識別符：RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-instance-public-access-check

檢查 Amazon Relational Database Service (Amazon RDS) 執行個體是否無法公開存取。如果執行個體組態項目的 publiclyAccessible 欄位為 true，則表示規則為「NON_COMPLIANT」。

Identifier: (識別符：) RDS_INSTANCE_PUBLIC_ACCESS_CHECK

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-in-backup-plan

檢查 AWS Backup 計劃中是否有 Amazon Relational Database Service (Amazon RDS) 資料庫。如果 Amazon RDS 資料庫未包含在任何 B AWS ackup 計劃中，則該規則為「不符合 _ 規範」。

> **Note**
>
> 此規則僅適用於 Amazon Aurora 資料庫執行個體。不支援 DB 叢集。

識別符：RDS_IN_BACKUP_PLAN

資源類型：AWS::RDS::DBInstance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-last-backup-recovery-point-created

檢查是否為 Amazon Relational Database Service (Amazon RDS) 建立復原點。如果 Amazon RDS 執行個體沒有在指定期限內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型：AWS::RDS::DBInstance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon RDS 執行個體標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon RDS 執行個體 ID。

恢復PointAgeValue（可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit（可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-logging-enabled

檢查是否已啟用 Amazon Relational Database Service (Amazon RDS) 的個別日誌。如果未啟用任何日誌類型，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 不處於 'available'、'backing-up'、'storage-optimization' 或 'storage-full'狀態的資料庫執行個體會評估為 `NOT_APPLICABLE`。

識別符： RDS_LOGGING_ENABLED

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

additionalLogs (選用), 類型: StringMap

以逗號分隔的引擎名稱和日誌類型名稱清單。例如，"additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-meets-restore-time-target

確認 Amazon RecalDatabase Service (Amazon RDS) 執行個體的還原時間是否符合指定的持續時間。如果 Amazon RDS 執行個體的時間超 maxRestoreTime 過 LatestRestoreExecutionTimeMinutes 分鐘，則該規則為「不相容」。

識別碼：RDS_MEETS_RESTORE_TIME_TARGET

資源類型：AWS::RDS::DBInstance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 Amazon RDS 執行個體標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon RDS 執行個體 ID。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-multi-az-support

檢查 RDS 資料庫執行個體是否啟用高可用性。

在異地同步備份部署中，Amazon RDS 會自動佈建，並在不同的可用區域中維持同步待命複本。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的高可用性 (多可用區域)。

> **Note**
>
> 此規則不會評估 Amazon Aurora 資料庫、Amazon DocumentDB 和 Amazon Neptune DB 執行個體。

識別符：RDS_MULTI_AZ_SUPPORT

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* 如需有關這些輸入有效值的詳細資訊，請參閱 AWS CloudFormation 使用指南中的 MultiAZ 和引擎。

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-resources-protected-by-backup-plan

檢查 Amazon Relational Database Service (Amazon RDS) 執行個體是否受備份計畫保護。如果備份計畫未涵蓋 Amazon RDS 資料庫執行個體，則表示規則為「NON_COMPLIANT」。

識別符：RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型：AWS::RDS::DBInstance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon RDS 執行個體標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon RDS 執行個體 ID。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （ 可選 ）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-snapshots-public-prohibited

檢查 Amazon Relational Database Service (Amazon RDS) 是否為公有狀態。如果任何現有和新的 Amazon RDS 快照為公有狀態，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 最多可能需要 12 小時才會擷取合規結果。

識別符：RDS_SNAPSHOTS_PUBLIC_PROHIBITED

資源類型:AWS:: RDS:: 資料庫快照，AWS:: RDS: 資料庫 ClusterSnapshot

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-snapshot-encrypted

檢查 Amazon Relational Database Service (Amazon RDS) DB 快照是否已加密。如果 Amazon RDS DB 快照未加密，則表示規則為「NON_COMPLIANT」。

識別碼：RDS_SNAPSHOT_ENCRYPTED

資源類型:AWS:: RDS:: 資料庫快照，AWS:: RDS: 資料庫 ClusterSnapshot

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## rds-storage-encrypted

檢查 Amazon Relational Database Service (Amazon RDS) DB 執行個體是否已啟用儲存加密功能。如果未啟用儲存加密功能，則表示規則為「NON_COMPLIANT」。

識別符：RDS_STORAGE_ENCRYPTED

資源類型：AWS::RDS::DBInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyId (選擇性), 類型：字串

用於加密儲存的 Amazon Resource Name (ARN) ID。

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-audit-logging-enabled

檢查 Amazon Redshift 叢集是否正在記錄特定儲存貯體的稽核。如果 Redshift 叢集未啟用稽核記錄，或者如果提供了 'bucketNames' 參數，但稽核記錄目的地不相符，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_AUDIT_LOGGING_ENABLED

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

bucketNames (選用), 類型：CSV

以逗號分隔的 Amazon S3 儲存貯體名稱清單，用於存放稽核日誌。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-backup-enabled

檢查是否已針對叢集啟用 Amazon Redshift 自動快照。如果 `automatedSnapshotRetentionPeriod` 的值大於 `MaxRetentionPeriod`、小於 `MinRetentionPeriod` 或值為 0，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_BACKUP_ENABLED

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

MinRetentionPeriod (選擇性), 類型：int

保留期間的最小值。最小值為 1。

MaxRetentionPeriod (選擇性), 類型：int

保留期間的最大值。最大值為 35。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-cluster-configuration-check

檢查 Amazon Redshift 叢集是否具有指定的設定。如果 Amazon Redshift 叢集未加密或使用其他金鑰加密，或者叢集未啟用稽核記錄，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_CLUSTER_CONFIGURATION_CHECK

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

集群 DbEncrypted, 類型：布林值, 預設：true

資料庫加密已啟用。

loggingEnabled, 類型：布林值, 預設：true

稽核記錄已啟用。

nodeTypes (選用), 類型：CSV, 預設：dc1.large

指定節點類型。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-cluster-kms-enabled

檢查 Amazon Redshift 叢集是否使用指定的 AWS Key Management Service (AWS KMS) 金鑰進行加密。如果已啟用加密，且使用 `kmsKeyArn` 參數中提供的金鑰對叢集進行加密，則表示規則為「COMPLIANT」。如果叢集未加密或使用其他金鑰加密，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_CLUSTER_KMS_ENABLED

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：CSV

以逗號分隔的 Amazon 紅移叢集中用於加 AWS KMS 密的金鑰亞馬遜資源名稱 (ARN) 清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-cluster-maintenancesettings-check

檢查 Amazon Redshift 叢集是否擁有指定的維護設定。如果停用自動升級主要版本，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

允許 VersionUpgrade, 類型：布林值, 預設：true

允許版本升級已啟用。

preferredMaintenanceWindow (選擇性), 類型：字串

叢集的排程維護時段 (例如，Mon:09:30-Mon:10:00)。

自動化 SnapshotRetentionPeriod (選擇性), 類型：int, 預設：1

保留自動快照的天數。

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
```

```
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* 如需有關這些輸入有效值的詳細資訊 AutomatedSnapshotRetentionPeriod，請參閱《 AWS CloudFormation 使用指南》中的〈PreferredMaintenance視窗〉和〈AllowVersion升級〉。

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-cluster-public-access-check

檢查 Amazon Redshift 叢集是否無法公開存取。如果叢集組態項目的 publiclyAccessible 欄位為 true，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
```

```
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-default-admin-check

檢查 Amazon Redshift 叢集是否已將管理員使用者名稱變更為其預設值。如果 Redshift 叢集的管理員使用者名稱設定為 “awsuser”，或者使用者名稱與參數中列出的內容不相符，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_DEFAULT_ADMIN_CHECK

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

有效AdminUserNames （ 可選 ），類型：CSV

Redshift 叢集要使用的管理員使用者名稱清單 (以逗號分隔)。注意：'awsuser' 是不接受的預設值。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-default-db-name-check

檢查 Redshift 叢集是否已從預設值變更其資料庫名稱。如果 Redshift 叢集的資料庫名稱設定為 “dev”，或者如果提供了選用參數且資料庫名稱不相符，則表示規則為「NON_COMPLIANT」。

識別符：REDSHIFT_DEFAULT_DB_NAME_CHECK

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

validDatabaseNames (選擇性), 類型：CSV

Redshift 叢集的資料庫名稱清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-enhanced-vpc-routing-enabled

檢查 Amazon Redshift 叢集是否已啟用「增強VpcRouting」。如果未啟用「增強VpcRouting」或設定，則該規則為「NON_COMPON_」。 enhancedVpcRouting 字段是 '假'。

識別符：REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

資源類型： AWS::Redshift::Cluster

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## redshift-require-tls-ssl

檢查 Amazon Redshift 叢集是否需要 TLS/SSL 加密才能連線至 SQL 用戶端。如果有任何 Amazon Redshift 叢集的 require_SSL 參數未設定為 true，則表示規則為「NON_COMPLIANT」。

識別碼：REDSHIFT_REQUIRE_TLS_SSL

資源類型: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter群組

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 無限制的紅移連接埠存取

檢查與 Amazon Redshift 叢集關聯的安全群組是否具有允許不受限制傳入流量的輸入規則。如果有輸入規則允許不受限制的傳入流量到 Redshift 叢集連接埠，則該規則為「不相容」。

標識符：密碼 _ 未限制 _ 端口 _ 訪問

資源類型： AWS::Redshift::Cluster

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## required-tags

檢查您的資源是否擁有指定的標籤。例如，您可以檢查 Amazon EC2 執行個體是否擁有 `CostCenter` 標籤，同時檢查所有 RDS 執行個體是否擁有一組金鑰標籤。以逗號分隔多個值。您一次最多可以檢查 6 個標籤。

AWS受管理的 AWS Systems Manager 自動化文件`AWS-SetRequiredTags`不適用於此規則的修正。您需要建立自己的自訂 Systems Manager 自動化文件以進行修復。

內容： AWS 可讓您以標籤形式將中繼 AWS 資料指派給資源。每個標籤 (tag) 都是由金鑰和選用值組成的標籤 (label)，用於儲存該資源上所保留資源或資料的資訊。如需詳細資訊，請參閱《擬定您的標記策略》。

您可以使用此規則，透過指定哪些資源應具有標籤及每個標籤的預期值，以尋找帳戶中未使用所需組態來啟動的資源。您也可以執行修復動作來修正標記錯誤。但是，此規則不會阻止您使用不正確的標籤建立資源。

識別符：REQUIRED_TAGS

資源類型 AWS::ACM::Certificate, AWS::AutoScaling:: AutoScaling 群組,: AWS::CloudFormation::Stack, AWS::CodeBuild: 專案,, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway,, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoad 平衡::LoadBalancer,,, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter 群組, AWS::Redshift::ClusterSecurity 群組, AWS::Redshift::ClusterSubnet 群組 AWS::Redshift::ClusterSnapshot, AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

tag1Key, 類型：字串, 預設值： CostCenter

必要標籤的索引鍵。

tag1Value (選用), 類型：CSV

必要標籤的選用值。以逗號分隔多個值。

tag2Key (選用), 類型：字串

第二個必要標籤的金鑰。

tag2Value (選用), 類型：CSV

第二個必要標籤的選用值。以逗號分隔多個值。

tag3Key (選用), 類型：字串

第三個必要標籤的金鑰。

tag3Value (選用), 類型：CSV

第三個必要標籤的選用值。以逗號分隔多個值。

tag4Key (選用), 類型：字串

第四個必要標籤的金鑰。

tag4Value (選用), 類型：CSV

第四個必要標籤的選用值。以逗號分隔多個值。

tag5Key (選用), 類型：字串

第五個必要標籤的金鑰。

tag5Value (選用), 類型：CSV

第五個必要標籤的選用值。以逗號分隔多個值。

tag6Key (選用), 類型：字串

第六個必要標籤的金鑰。

tag6Value (選用), 類型：CSV

第六個必要標籤的選用值。以逗號分隔多個值。

## AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## restricted-common-ports

> **Important**
>
> 針對此規則，規則識別符 (RESTRICTED_INCOMING_TRAFFIC) 和規則名稱 (restricted-common-ports) 不同。

檢查使用中的安全性群組是否不允許連入到指定連接埠的傳輸控制通訊協定 (TCP) 的不受限制流量。在下列情況下，規則為「COMPLIANT」：

- 已封鎖所有 TCP 流量的連接埠存取。
- TCP 流量的連接埠存取是透過輸入規則開放，其中來源可以是單一 IPv4 位址或 CIDR 標記法中的一個 IPv4 位址範圍，但不涵蓋所有 IPv4 位址 ("0.0.0.0/0")。
- TCP 流量的連接埠存取是透過輸入規則開放，其中來源可以是單一 IPv6 位址或 CIDR 標記法中的一個 IPv6 位址範圍，但不涵蓋所有 IPv6 位址 ("::/0)")。

如果傳入 TCP 連線的 IP 位址不限於指定的連接埠，則該規則為「NON_COMPLIANT」。

識別符：RESTRICTED_INCOMING_TRAFFIC

資源類型： AWS::EC2::SecurityGroup

觸發類型： Configuration changes (組態變更) 和 Periodic (定期)。

AWS 區域：所有支援的 AWS 地區

參數：

blockedPort1 (選用), 類型：int, 預設：20

已封鎖的 TCP 連接埠號碼。20 的預設值對應於檔案傳輸通訊協定 (FTP) 資料傳輸。

blockedPort2 (選用), 類型：int, 預設：21

已封鎖的 TCP 連接埠號碼。21 的預設值對應於檔案傳輸通訊協定 (FTP) 命令控制。

blockedPort3 (選用), 類型：int, 預設：3389

已封鎖的 TCP 連接埠號碼。3389 的預設值對應於遠端桌面通訊協定 (RDP)。

blockedPort4 (選用), 類型：int, 預設：3306

已封鎖的 TCP 連接埠號碼。3306 的預設值對應於 MySQL 通訊協定。

blockedPort5 (選用), 類型：int, 預設：4333

已封鎖的 TCP 連接埠號碼。4333 的預設值對應於 MySQL 通訊協定。

blockedPorts (選用), 類型：CSV

以逗號分隔的封鎖 TCP 連接埠號清單。例如，20、21、3306、3389 和 4333。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## root-account-hardware-mfa-enabled

檢查您的 AWS 帳戶是否已啟用使用多因素身份驗證（MFA）硬件設備以 root 身份證明登錄。如果允許任何虛擬 MFA 裝置使用根登入資料登入，則表示規則為 NON_COMPLIANT。

> **Note**
>
> 受管規則和全域 IAM 資源類型
> 2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
> 如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
> 為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

Identifier: (識別符：) ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## root-account-mfa-enabled

檢查您帳戶的 root 用 AWS 戶是否需要進行控制台登錄的多因素身份驗證。如果 AWS Identity and Access Management (IAM) 根帳戶使用者未啟用多因素驗證 (MFA)，則該規則為 NON_COMPOFIT。

> **Note**
>
> 受管規則和全域 IAM 資源類型
> 2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。
> 如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。
> 為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

識別符：ROOT_ACCOUNT_MFA_ENABLED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## route53-query-logging-enabled

檢查您的 Amazon Route 53 公有託管區域是否已啟用 DNS 查詢日誌記錄。如果您的 Amazon Route 53 公有託管區域未啟用 DNS 查詢日誌記錄，則表示規則為「NON_COMPLIANT」。

識別符：ROUTE53_QUERY_LOGGING_ENABLED

資源類型： AWS::Route53::HostedZone

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-access-point-in-vpc-only

檢查 Amazon S3 存取點是否不允許從網際網路存取 (NetworkOrigin 即 VPC)。如 NetworkOrigin 果是網際網路，則該規則為「不符合 _」。

識別符：S3_ACCESS_POINT_IN_VPC_ONLY

資源類型： AWS::S3::AccessPoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-access-point-public-access-blocks

檢查 Amazon S3 Access Points 是否已啟用封鎖公開存取設定。如果未針對 S3 存取點啟用封鎖公開存取設定，則表示規則為「NON_COMPLIANT」。

識別符：S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

資源類型： AWS::S3::AccessPoint

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

excludedAccessPoints (選擇性), 類型：CSV

允許的公有 Amazon S3 Access Points 名稱清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-account-level-public-access-blocks

檢查是否已從帳戶層級設定所需的公有存取權封鎖設定。僅在以下設定的欄位與組態項目中的對應欄位不符時，規則才為 NON_COMPLIANT。

> **Note**
>
> 如果您使用此規則，請確定已啟用 S3 封鎖公有存取權。規則為「變更觸發」，因此除非啟用 S3 封鎖公有存取權，否則不會調用規則。如果未啟用 S3 封鎖公有存取權，則規則會傳回

「INSUFFICIENT_DATA」。這意味著您仍然可能有一些公有儲存貯體。如需設定 S3 封鎖公有存取權的詳細資訊，請參閱《封鎖 Amazon S3 儲存的公有存取權》。

識別符：S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

資源類型： AWS::S3::AccountPublicAccessBlock

觸發類型：組態變更 (未核取目前狀態，只有在變更產生新事件時才評估)

> **Note**
>
> 此規則只會由 S3 端點所在之特定區域的組態變更所觸發。在所有其他區域中，規則會受到定期檢查。如果在其他區域中進行了變更，則在規則傳回「NON_COMPLIANT」之前可能會出現延遲。

AWS 區域：所有支援的 AWS 地區

參數：

IgnorePublicAcls (選擇性), 類型：字串, 預設：True

IgnorePublicAcls 是否強制執行，預設為 True

BlockPublicPolicy (選擇性), 類型：字串, 預設：True

BlockPublicPolicy 是否強制執行，預設為 True

BlockPublicAcls (選擇性), 類型：字串, 預設：True

BlockPublicAcls 是否強制執行，預設為 True

RestrictPublicBuckets (選擇性), 類型：字串, 預設：True

RestrictPublicBuckets 是否強制執行，預設為 True

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-account-level-public-access-blocks-periodic

檢查是否已從帳戶層級設定所需的公有存取封鎖設定。如果組態項目與參數 (或預設值) 中的一或多個設定不相符，則表示規則為「NON_COMPLIANT」。

識別符：S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

IgnorePublicAcls (選擇性), 類型：字串

IgnorePublicAcls 是否強制執行，預設為 True

BlockPublicPolicy (選擇性), 類型：字串

BlockPublicPolicy 是否強制執行，預設為 True

BlockPublicAcls (選擇性), 類型：字串

BlockPublicAcls 是否強制執行，預設為 True

RestrictPublicBuckets (選擇性), 類型：字串

RestrictPublicBuckets 是否強制執行，預設為 True

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-acl-prohibited

檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體是否透過存取控制清單 (ACL) 允許使用者的許可。如果針對 Amazon S3 儲存貯體中的使用者存取設定 ACL，則表示規則為「NON_COMPLIANT」。

識別符：S3_BUCKET_ACL_PROHIBITED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-blacklisted-actions-prohibited

檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策是否不允許針對來自其他帳戶的主體對儲存貯體中的資源進行區塊層級和物件層級動作。 AWS 例如，規則會檢查 Amazon S3 儲存貯體政策不允許其他 AWS 帳戶對儲存貯體中的任何物件執行任何`s3:GetBucket*`動作。`s3:DeleteObject`如果 Amazon S3 儲存貯體政策允許任何列入封鎖名單的動作，則表示規則為「NON_COMPLIANT」。

> **Note**
> 此規則只會檢查主體屬性中的實體，而不會考量政策中「條件」屬性下的任何條件

識別符：S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

列入黑名單 ActionPattern, 類型：CSV

以逗號分隔的黑名單動作模式清單，例如 s3: GetBucket * 和 s3:。DeleteObject

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 啟用 S3 儲存區跨區域複寫

檢查您是否已為 Amazon S3 儲存貯體啟用 S3 跨區域複寫。如果沒有啟用跨區域複寫的複寫規則，則該規則為「NON_COLUTION」。

識別碼：S3_ 桶 _ 交叉 _ 區域 _ 複製 _ 啟用

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-default-lock-enabled

檢查 S3 儲存貯體是否預設已啟用鎖定。如果鎖定未啟用，則表示規則為「NON_COMPLIANT」。

識別碼： S3_BUCKET_DEFAULT_LOCK_ENABLED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

mode (選用), 類型：字串

模式：(選用) 具有有效值 GOVERNANCE 或 COMPLIANCE 的模式參數。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-level-public-access-prohibited

檢查 S3 儲存貯體是否可公開存取。如果 `excludedPublicBuckets` 參數中未列出 S3 儲存貯體，且儲存貯體層級設定為公有，則表示規則為「NON_COMPLIANT」。

識別符：S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

excludedPublicBuckets (選擇性), 類型：CSV

已知允許的公有 Amazon S3 儲存貯體名稱清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-logging-enabled

檢查 S3 儲存貯體是否已啟用日誌記錄。如果未啟用日誌記錄，則規則為「NON_COMPLIANT」。

識別符：S3_BUCKET_LOGGING_ENABLED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

targetBucket (選用), 類型：字串

儲存伺服器存取記錄的目標 S3 儲存貯體。

targetPrefix (選用), 類型：字串

儲存伺服器存取日誌的 S3 儲存貯體字首。

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "BucketName": "my-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "my-log-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-mfa-delete-enabled

檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制組態是否已啟用 MFA 刪除功能。如果未啟用 MFA 刪除功能，則表示規則為「NON_COMPLIANT」。

識別符：S3_BUCKET_MFA_DELETE_ENABLED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-policy-grantee-check

檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 VPC 的限制。如果儲存貯體政策不存在，則表示規則為 COMPLIANT。

例如，如果規則的輸入參數是兩個委託人清單：111122223333 和 444455556666 且儲存貯體政策指定只有 111122223333 可以存取儲存貯體，則表示規則為 COMPLIANT。使用相同的輸入參數：如果儲存貯體政策指定 111122223333 和 444455556666 可存取儲存貯體，則規則也合規。不過，如果儲存貯體政策指定 999900009999 可以存取儲存貯體，則表示規則為 NON-COMPLIANT。

> **Note**
>
> 如果儲存貯體政策包含多個陳述式，則儲存貯體政策中的每個陳述式都會根據此規則進行評估。

Identifier: (識別符：) S3_BUCKET_POLICY_GRANTEE_CHECK

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

awsPrincipals (選用), 類型：CSV

以逗號分隔的主體清單，例如 IAM 使用者 ARN、IAM 角色 ARN 和 AWS 帳戶，例如「arn: aw:iam::: 11112222333: 使用者/愛麗絲，雲:: aw: IAM:: 444455556666: 角色/鮑勃, 123456789012'。

servicePrincipals (選用), 類型：CSV

以逗號分隔的服務主體清單，例如 'cloudtrail.amazonaws.com, lambda.amazonaws.com'。

federatedUsers (選用), 類型：CSV

以逗號分隔之 Web 聯合身分的身分提供者清單，例如 Amazon Cognito 和 SAML 身分提供者。例如 'cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider'。

ipAddresses (選用), 類型：CSV

以逗號分隔的 CIDR 格式化 IP 地址清單，例如 '10.0.0.1, 192.168.1.0/24, 2001:db8::/32'。

vpcIds (選用), 類型：CSV

以逗號分隔的 Amazon Virtual Private Cloud (Amazon VPC) ID 清單，例如 'vpc-1234abc0, vpc-ab1234c0'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-policy-not-more-permissive

確認除了您提供的控制 Amazon S3 儲存貯體政策，您的 Amazon Simple Storage Service 儲存貯體政策不允許任何其他跨帳戶許可。

> **Note**
> 如果您提供的參數值無效，您會看到下列錯誤：controlPolicy 參數的值必須是 Amazon S3 儲存貯體政策。

識別符：S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

controlPolicy, 類型：字串

定義 S3 儲存貯體許可上限的 Amazon S3 儲存貯體政策。政策長度上限為 1024 個字元。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-public-read-prohibited

檢查您的 Amazon S3 儲存貯體是否不允許公開讀取存取。規則會檢查封鎖公開存取設定、儲存貯體政策和儲存貯體存取控制清單 (ACL)。

同時滿足以下兩個條件時，規則是合規的：

- 封鎖公開存取設定限制公有政策或儲存貯體政策不允許公有讀取存取。
- 封鎖公開存取設定限制公有 ACL 或儲存貯體 ACL 不允許公有讀取存取。

在以下情況，規則不合規：

- 如果 [封鎖公用存取] 設定未限制公用原則，請 AWS Config 評估原則是否允許公用讀取存取。如果政策允許公有讀取存取，表示規則不合規。
- 如果「封鎖公用存取」設定未限制公用值區 ACL，請 AWS Config 評估值區 ACL 是否允許公開讀取存取。如果儲存貯體 ACL 允許公有讀取存取，表示規則不合規。

識別符：S3_BUCKET_PUBLIC_READ_PROHIBITED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更) 和 Periodic (定期)。

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-public-write-prohibited

檢查您的 Amazon S3 儲存貯體是否不允許公有寫入存取。規則會檢查封鎖公開存取設定、儲存貯體政策和儲存貯體存取控制清單 (ACL)。

同時滿足以下兩個條件時，規則是合規的：

- 封鎖公開存取設定限制公有政策或儲存貯體政策不允許公有寫入存取。
- 封鎖公開存取設定限制公有 ACL 或儲存貯體 ACL 不允許公有寫入存取。

在以下情況，規則不合規：

- 如果 [封鎖公用存取] 設定未限制公用原則，請 AWS Config 評估原則是否允許公用寫入存取。如果政策允許公有寫入存取，表示規則不合規。
- 如果「封鎖公用存取」設定未限制公用值區 ACL，請 AWS Config 評估值區 ACL 是否允許公開寫入存取。如果儲存貯體 ACL 允許公有寫入存取，表示規則不合規。

> **Note**
>
> 此規則不會評估帳戶層級公有封鎖存取的變更。若要檢查是否從帳戶層級設定了所需的公有存取封鎖設定，請參閱 s3-account-level-public-access-blocks 和 s3-account-level-public-access-blocks-periodic。

識別符：S3_BUCKET_PUBLIC_WRITE_PROHIBITED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更) 和 Periodic (定期)。

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-replication-enabled

檢查 S3 儲存貯體是否已啟用複寫規則。如果 S3 儲存貯體沒有複寫規則或具有未啟用的複寫規則，則表示規則為「NON_COMPLIANT」。

識別符：S3_BUCKET_REPLICATION_ENABLED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

ReplicationType (選擇性), 類型：字串

> 接受的值：'CROSS-REGION' 和 'SAME-REGION'。針對規則輸入 'CROSS-REGION'，以檢查所有儲存貯體是否僅啟用跨區域複寫。針對規則輸入 'SAME-REGION'，以檢查所有儲存貯體是否僅啟用相同區域複寫。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-server-side-encryption-enabled

檢查您的 Amazon S3 儲存貯體已啟用 Amazon S3 預設加密，或 S3 儲存貯體政策明確拒絕不需使用 AES-256 或 AWS Key Management Service伺服器端加密的 `put-object` 請求。如果您的 Amazon S3 儲存貯體預設為未加密，則表示規則為「NON_COMPLIANT」。

識別符：S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-ssl-requests-only

檢查 S3 儲存貯體是否有需要請求使用 SSL/TLS 的政策。如果任何 S3 儲存貯體具有允許 HTTP 請求的政策，則表示規則為「NON_COMPLIANT」。

識別符：S3_BUCKET_SSL_REQUESTS_ONLY

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-bucket-versioning-enabled

檢查是否已啟用 S3 儲存貯體的版本控制。規則會選擇性檢查 S3 儲存貯體的 MFA 刪除是否啟用。

識別符：S3_BUCKET_VERSIONING_ENABLED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

是 MfaDeleteEnabled (選擇性), 類型：字串

S3 儲存貯體已啟用 MFA 刪除。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-default-encryption-kms

檢查 S3 儲存貯體是否使用金 AWS 鑰管理服務 (AWS KMS) 加密。如果 S3 儲存貯體未使用 AWS KMS 金鑰加密，則該規則為「不相容」。

識別碼： S3_DEFAULT_ENCRYPTION_KMS

資源類型: AWS::S3::Bucket, AWS::KMS::Key

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：CSV

允許加密 Amazon S3 儲存貯體的 AWS KMS 金鑰 ARN 清單 (逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-event-notifications-enabled

檢查是否在 S3 儲存貯體上啟用 Amazon S3 事件通知。如果儲存貯體上未設定 S3 事件通知，或者事件類型或目的地與 `eventTypes` 和 destinationArn 參數不相符，則表示規則為「NON_COMPLIANT」。

識別符：S3_EVENT_NOTIFICATIONS_ENABLED

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

destinationArn (選用), 類型：字串

事件通知目的地的 Amazon 資源名稱 (ARN) (Amazon SNS 主題、 AWS Lambda、Amazon SQS 佇列)。

eventTypes (選用), 類型：CSV

以逗號分隔的偏好 Amazon S3 事件類型清單

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-last-backup-recovery-point-created

檢查是否已為 Amazon Simple Storage Service (Amazon S3) 建立復原點。如果 Amazon S3 儲存貯體沒有在指定期間內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：S3_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::S3::Bucket

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon S3 儲存貯體標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon S3 儲存貯體名稱。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-lifecycle-policy-check

檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體是否已設定生命週期規則。如果沒有使用中的生命週期組態規則或組態與參數值不相符，則表示規則為「NON_COMPLIANT」。

識別符：S3_LIFECYCLE_POLICY_CHECK

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

targetTransitionDays (選擇性), 類型：int

指示物件在建立後轉換成指定儲存類別的天數 (例如 30 天)。

targetExpirationDays (選擇性), 類型：int

物件在建立後受到刪除的天數 (例如 395 天)。

目標 TransitionStorageClass (選擇性), 類型：字串

目的地儲存類別類型 (例如，Amazon S3 Standard-Infrequent Access (S3 Standard-IA))。如需詳細資訊，請參閱 https: //docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html。

targetPrefix (選用), 類型：字串

用於識別一或多個物件的 Amazon S3 物件字首。

bucketNames (選用), 類型：CSV

啟用生命週期政策的 Amazon S3 儲存貯體名稱清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-meets-restore-time-target

確認 Amazon Simple Storage Service (Amazon S3) 儲存貯體的還原時間是否符合指定的持續時間。如果 Amazon S3 儲存貯體大於 LatestRestoreExecutionTimeMinutes maxRestoreTime 分鐘，則該規則為「不符合」規則。

識別碼：S3_MEETS_RESTORE_TIME_TARGET

資源類型： AWS::S3::Bucket

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大 RestoreTime, 類型：int

允許的還原執行期上限數值。

resourceTags (選用), 類型：字串

規則中需檢查的 Amazon S3 儲存貯體標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon S3 儲存貯體名稱。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-resources-protected-by-backup-plan

檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體是否受備份計畫保護。如果備份計畫未涵蓋 Amazon S3 儲存貯體，則表示規則為「NON_COMPLIANT」。

識別符：S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::S3::Bucket

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Amazon S3 儲存貯體標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則中需檢查的 Amazon S3 儲存貯體名稱。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

### AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## s3-version-lifecycle-policy-check

檢查 Amazon Simple Storage Service (Amazon S3) 版本的已啟用儲存貯體是否已設定生命週期政策。如果未啟用 Amazon S3 生命週期政策，則表示規則為「NON_COMPLIANT」。

識別符：S3_VERSION_LIFECYCLE_POLICY_CHECK

資源類型： AWS::S3::Bucket

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

bucketNames (選用), 類型：CSV

啟用生命週期政策的 Amazon S3 儲存貯體名稱清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## sagemaker-endpoint-configuration-kms-key-configured

檢查金 AWS 鑰管理服務 (AWS KMS) 金鑰是否已針對 Amazon SageMaker 端點組態設定。如果未針對 Amazon SageMaker 端點組態指定「KmsKeyId'」，則該規則為「不符合」規則。

識別符：SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

資源類型： AWS::SageMaker::EndpointConfig

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：字串

Amazon SageMaker 端點組態允許的特定 AWS KMS 金鑰 ARN 的逗號分隔清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 命形器-端點配置-配置-實例計數

檢查 Amazon SageMaker 端點組態是否將生產變體「InitialInstanceCount`」設定為大於 1 的值。如果生產變體「InitialInstance計數」等於 1，則規則為「不相容」。

識別碼：箭頭端點 _ 組態 _ 實例計數

資源類型： AWS::SageMaker::EndpointConfig

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## sagemaker-notebook-instance-inside-vpc

檢查 Amazon SageMaker 筆記本執行個體是在 VPC 內還是核准子網路清單中啟動。如果筆記本執行個體未在 VPC 中啟動，或者其子網路 ID 未包含在參數清單中，則表示規則為「NON_COMPLIANT」。

識別符：SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

資源類型： AWS::SageMaker::NotebookInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

SubnetIds (選擇性), 類型：CSV

可在其中啟動筆記本執行個體的子網路 ID 清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## sagemaker-notebook-instance-kms-key-configured

檢查 Amazon SageMaker 筆記本執行個體是否已設定金 AWS 鑰管理服務 (AWS KMS) 金鑰。如果未為筆記本執行個體指定 'KmsKeyId'，則規則為「NON_ 相容」。 SageMaker

識別符： SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

資源類型： AWS::SageMaker::NotebookInstance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：字串

Amazon SageMaker 筆記本執行個體允許使用逗號分隔的 AWS KMS 金鑰 ARN 清單。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## sagemaker-notebook-instance-root-access-check

檢查 Amazon SageMaker 筆記本執行個體是否已啟用 Amazon SageMaker RootAccess 設定。如果 Amazon SageMaker 筆記本執行個體的 RootAccess 設定設為「啟用」，則該規則為「不符合」規則。

識別符：SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

資源類型： AWS::SageMaker::NotebookInstance

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## sagemaker-notebook-no-direct-internet-access

檢查 Amazon SageMaker 筆記型電腦執行個體是否已停用直接網際網路存取。如果 SageMaker 筆記本執行個體已啟用網際網路，則該規則為「NON_ 相容」

識別符： SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

資源類型： AWS::SageMaker::NotebookInstance

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## secretsmanager-rotation-enabled-check

檢查 AWS 密碼管理員密碼是否已啟用輪換。規則也會檢查選用的 `maximumAllowedRotationFrequency` 參數。如果指定了參數，則秘密的輪換頻率將會與允許的頻率上限進行比較。如果未排定輪換秘密，表示規則為 NON_COMPLIANT。如果旋轉頻率高於「頻率」參數中指定的數字，則該規則也是「NON_ 相容」 maximumAllowedRotation。

> **Note**
>
> 在第一次評估的 4 小時內重新評估此規則，對結果沒有任何影響。

識別符：SECRETSMANAGER_ROTATION_ENABLED_CHECK

資源類型： AWS::SecretsManager::Secret

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

最大值 AllowedRotationFrequency (選擇性), 類型：int

允許的秘密輪換頻率上限 (以天為單位)。

最大值 AllowedRotationFrequencyInHours (選擇性), 類型：int

允許的密碼輪換頻率上限 (以小時為單位)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## secretsmanager-scheduled-rotation-success-check

檢查 AWS Secrets Manager 密碼是否根據循環排程順利輪換。Secrets Manager 可計算輪換應該進行的日期。如果該日已過且密碼未輪換，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 規則會針對沒有輪換的密碼傳回「NOT_APPLICABLE」。

識別符：SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

資源類型： AWS::SecretsManager::Secret

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## secretsmanager-secret-periodic-rotation

檢查 AWS Secrets Manager 密碼是否在過去指定的天數內輪替。如果密碼的 maxDaysSince輪換天數超過循環天數，則規則為「不符合 N_COMPON_」。預設值為 90 天。

識別符：SECRETSMANAGER_SECRET_PERIODIC_ROTATION

資源類型： AWS::SecretsManager::Secret

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

最大DaysSinceRotation （可選），類型：int

密碼可以保持不變的天數上限。預設值為 90 天。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## secretsmanager-secret-unused

檢查 AWS Secrets Manager 密碼是否在指定天數內被存取。如果在「未使用」的天數內未存取密碼，則該規則為「NON_COMPON_ForDays」。預設值為 90 天。

內容：建議您定期刪除未使用的密碼。不再需要存取這些密碼的先前使用者可能會誤用未使用的密碼。此外，隨著越來越多使用者獲得密碼的存取權，其濫用密碼或被授予未經授權實體存取權限的可能性也越來越高。刪除未使用的密碼有助於向不再需要密碼存取權的使用者撤銷存取權，並可降低使用 AWS Secrets Manager的成本。

識別符：SECRETSMANAGER_SECRET_UNUSED

資源類型： AWS::SecretsManager::Secret

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

unusedForDays (選擇性), 類型：int

密碼可以保持為未使用的天數。預設值為 90 天。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## secretsmanager-using-cmk

檢查中的所有密碼 AWS Secrets Manager 是否使用 AWS 受管金鑰 (`aws/secretsmanager`) 或在 AWS Key Management Service (AWS KMS) 中建立的客戶管理金鑰加密。如果使用客戶自管金鑰加密密碼，則表示規則為「COMPLIANT」。如果使用 `aws/secretsmanager` 加密密碼，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則無法存取跨帳戶客戶自管金鑰，並在使用跨帳戶金鑰時將密碼評估為「NON_COMPLIANT」。

識別符：SECRETSMANAGER_USING_CMK

資源類型： AWS::SecretsManager::Secret

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyArns (選擇性), 類型：CSV

以逗號分隔的 KMS 金鑰 Amazon Resource Name (ARN) 清單，以檢查金鑰是否用於加密。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## securityhub-enabled

檢查 AWS 帳戶是否已啟用 AWS Security Hub。如果未啟用「 AWS Security Hub」，則該規則為「不相容」。

識別碼： SECURITYHUB_ENABLED

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## security-account-information-provided

檢查您是否已為 AWS 帳戶聯絡人提供安全性連絡人資訊。如果未提供帳戶內的安全性聯絡人資訊，則表示規則為「NON_COMPLIANT」。

識別符：SECURITY_ACCOUNT_INFORMATION_PROVIDED

資源類型：AWS::::Account

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 與組織內共用的服務目錄

在啟用「組織」的整合時，檢查「 AWS Service AWS Catalog」是否與組 Organizations 共用產品組合 (視為單一單位的 AWS 帳戶集合)。如果股份的「類型」值是「帳戶」，則該規則是「不符合 _」的規則。

識別碼：服務 _ 目錄 _ 與組織共用 _

資源類型： AWS::ServiceCatalog::Portfolio

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## service-vpc-endpoint-enabled

檢查是否為每個 Amazon Virtual Private Cloud (Amazon VPC) 所建立之規則參數中提供服務的服務端點。如果 Amazon VPC 沒有為該服務建立 Amazon VPC 端點，則表示規則為「NON_COMPLIANT」。

識別符：SERVICE_VPC_ENDPOINT_ENABLED

資源類型:AWS:: EC2:: VPC

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

serviceName, 類型：字串

服務的簡稱或尾碼。注意：若要取得可用服務名稱或有效尾碼清單的清單，請使用 DescribeVpcEndpointServices。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ses-malware-scanning-enabled

檢查 Amazon Simple Email Service (Amazon SES) 是否已啟用接收訊息時的惡意軟體和垃圾郵件掃描。如果未啟用惡意軟體和垃圾郵件掃描，則表示規則為「NON_COMPLIANT」。

識別符：SES_MALWARE_SCANNING_ENABLED

資源類型： AWS::SES::ReceiptRule

觸發類型：定期

AWS 區域：只有在歐洲 (愛爾蘭)、美國東部 (維吉尼亞北部)、美國西部 (奧勒岡) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## shield-advanced-enabled-autorenew

檢查您的 AWS 帳戶是否已啟用 AWS Shield Advanced，並且此訂閱設定為自動續訂。如果已啟用 Shield Advanced 和自動續約，則表示規則為「COMPLIANT」。

> **Note**
>
> 的 API 端點 AWS Shield Advanced 僅在美國東部 (維吉尼亞北部) 區域提供。此規則應只在美國東部 (維吉尼亞北部) 區域中排程執行。

識別符： SHIELD_ADVANCED_ENABLED_AUTORENEW

觸發類型：定期

AWS 區域：僅在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## shield-drt-access

檢查 Shield 牌回應小組 (SRT) 是否可以存取您的 AWS 帳戶。如果 AWS Shield Advanced 已啟用，但未設定 SRT 存取的角色，則該規則為「不相容」。

識別符： SHIELD_DRT_ACCESS

觸發類型：定期

AWS 區域：僅在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## sns-encrypted-kms

檢查 SNS 主題是否已使用金 AWS 鑰管理服務 (AWS KMS) 加密。如果 SNS 主題未使 AWS 用 KMS 加密，則該規則為「不相容」。或者，指定要檢查之規則的索引鍵 ARN、別名 ARN、別名名稱或索引鍵 ID。

識別碼： SNS_ENCRYPTED_KMS

資源類型： AWS::SNS::Topic

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

kmsKeyIds (選擇性), 類型：CSV

> 以逗號分隔的 AWS KMS 金鑰 Amazon 資源名稱 (ARN)、KMS 別名 ARN、KMS 別名或要檢查之規則的 KMS 金鑰識別碼清單。

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COMPANTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## sns-topic-message-delivery-notification-enabled

檢查傳送至端點主題的通知訊息交付狀態是否已啟用 Amazon Simple Notification Service (SNS) 記錄。如果未啟用訊息交付狀態通知，則表示規則為「NON_COMPLIANT」。

識別符：SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

資源類型： AWS::SNS::Topic

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## ssm-document-not-public

檢查帳戶所擁有的 AWS Systems Manager 文件是否公開。如果具有擁有者 'Self' 的 Systems Manager 文件為公有，則表示規則為「NON_COMPLIANT」。

識別符：SSM_DOCUMENT_NOT_PUBLIC

資源類型： AWS::SSM::Document

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## step-functions-state-machine-logging-enabled

檢查 AWS Step Functions 機器是否啟用了日誌記錄。如果狀態機器未啟用日誌記錄，或日誌記錄組態不在提供的最低層級，則表示規則為「NON_COMPLIANT」。

識別符：STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

資源類型： AWS::StepFunctions::StateMachine

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

雲端 WatchLogGroupArns (選擇性), 類型：CSV

Amazon CloudWatch 日誌記錄群組的 Amazon 資源名稱 (ARN) 清單 (逗號分隔)。此規則會檢查指定的日誌群組是否已針對您的狀態機器日誌進行設定。

logLevel (選用), 類型：字串

狀態機器的最低日誌層級。有效值包括：ALL、ERROR、FATAL。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## storagegateway-last-backup-recovery-point-created

檢查 S AWS torage Gateway 磁碟區是否已建立復原點。如果 Storage Gateway 磁碟區沒有在指定期間內建立對應的復原點，則表示規則為「NON_COMPLIANT」。

識別符：STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::StorageGateway::Volume

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Storage Gateway 磁碟區標籤，採用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId (選用), 類型：字串

規則要檢查的 Storage Gateway 磁碟區 ID。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## storagegateway-resources-protected-by-backup-plan

檢查 S AWS torage Gateway 磁碟區是否受備份計劃的保護。如果備份計畫未涵蓋 Storage Gateway 磁碟區，則表示規則為「NON_COMPLIANT」。

識別符：STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::StorageGateway::Volume

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

規則要檢查的 Storage Gateway 磁碟區標籤，採用 JSON 格式。

resourceId (選用), 類型：字串

規則要檢查的 Storage Gateway 磁碟區 ID。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （ 可選 ）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## subnet-auto-assign-public-ip-disabled

檢查 Amazon Virtual Private Cloud (Amazon VPC) 子網路是否獲指派公有 IP 地址。如果 Amazon VPC 沒有獲指派公有 IP 地址的子網路，則表示規則為「COMPLIANT」。如果 Amazon VPC 具有獲指派公有 IP 地址的子網路，則表示規則為「NON_COMPLIANT」。

識別符：SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

資源類型： AWS::EC2::Subnet

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

主動評估

有關如何在主動模式下執行此規則的步驟，請參閱使用 AWS Config 規則評估資源。若要讓此規則在主動模式下傳回 COLINTING，StartResource評估 API 的資源組態結構描述必須包含下列輸入 (編碼為字串)：

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

如需主動評估的詳細資訊，請參閱《評估模式》。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 傳輸家庭服務器-無 FTP

檢查使用 AWS Transfer Family 建立的伺服器是否使用 FTP 進行端點連線。如果端點連線的伺服器通訊協定已啟用 FTP，則該規則為「NON_ 相容」。

識別碼：傳輸 _ 家族 _ 伺服器 _NO_FTP

資源類型： AWS::Transfer::Server

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## virtualmachine-last-backup-recovery-point-created

檢查是否已為 AWS 備份 VirtualMachines閘道建立復原點。如果 AWS 備份閘道在指定期 VirtualMachines 間內沒有建立對應的復原點，則該規則為「NON_COLUTION」。

識別符：VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

資源類型： AWS::BackupGateway::VirtualMachine

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

要檢查之規則的 AWS 備 VirtualMachines 份閘道標記，採用 JSON 格式。`{"tagkey" : "tagValue"}`

resourceId (選用), 類型：字串

要檢查之規則的 AWS 備 VirtualMachine 份閘道識別碼。

恢復PointAgeValue （可選）, 類型：int, 預設：1

允許年齡上限的數值。小時不可超過 744 個小時，天數不可超過 31 天。

恢復PointAgeUnit （可選）, 類型：字串, 預設：天

允許年齡上限的時間單位。接受的值：'hours'、'days'。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## virtualmachine-resources-protected-by-backup-plan

檢查 AWS Backup 閘道 VirtualMachines 是否受備份計畫的保護。如果 Backup 閘道不在備份計畫涵蓋範圍內，則該規則 VirtualMachine 為「NON_ 相容」。

識別符：VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

資源類型： AWS::BackupGateway::VirtualMachine

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

resourceTags (選用), 類型：字串

要檢查之規則的 AWS 備 VirtualMachines 份閘道標籤，採用 JSON 格式。`{"tagkey" : "tagValue"}`

resourceId (選用), 類型：字串

要檢查之規則的 AWS 備 VirtualMachine 份閘道識別碼。

crossRegionList (選擇性), 類型：字串

跨區域備份副本要保留的目的地區域清單 (以逗號分隔)

crossAccountList (選擇性), 類型：字串

跨帳戶備份副本要保留的目標帳戶清單 (以逗號分隔)

maxRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最長保留期 (以天為單位)

minRetentionDays (選擇性), 類型：int

備份保存庫鎖定的最短保留期間 (以天為單位)

備份VaultLockCheck （可選）, 類型：字串

接受的值：'True' 或 'False'。針對規則輸入 'True'，以檢查資源是否已在鎖定的保存庫中備份

### AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## vpc-default-security-group-closed

檢查是否任何 Amazon Virtual Private Cloud (Amazon VPC) 的預設安全群組皆不允許傳入或傳出流量。如果預設安全群組包含一或多個傳入或傳出流量規則，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> AWS Config 記錄刪除相關資源 (例如預設安全群組) 刪除作為 Amazon VPC 刪除的一部分而刪除時，可能會有延遲。因此，即使已刪除或修復所有預設安全群組或其他相關資源，規則仍可能會報告「NON_COMPLIANT」，直到下一個帳戶基準程序為止。

Identifier: (識別符：) VPC_DEFAULT_SECURITY_GROUP_CLOSED

資源類型： AWS::EC2::SecurityGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## vpc-flow-logs-enabled

檢查是否已為所有 Amazon VPC 找到並啟用 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌。如果至少一個 Amazon VPC 沒有啟用流程日誌，則表示規則為「NON_COMPLIANT」。

Identifier: (識別符：) VPC_FLOW_LOGS_ENABLED

資源類型:AWS:: EC2:: VPC

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

trafficType (選用), 類型：字串

TrafficType 流程記錄

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## vpc-network-acl-unused-check

檢查是否有未使用的網路存取控制清單 (network ACL)。如果每個網路 ACL 都與子網路建立關聯，則表示規則為「COMPLIANT」。如果網路 ACL 未與子網路建立關聯，則表示規則為「NON_COMPLIANT」。

識別符：VPC_NETWORK_ACL_UNUSED_CHECK

資源類型： AWS::EC2::NetworkAcl

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## vpc-peering-dns-resolution-check

檢查是否已啟用從接受者/請求者 VPC 到私有 IP 的 DNS 解析。如果未啟用從接受者/請求者 VPC 到私有 IP 的 DNS 解析，則表示規則為「NON_COMPLIANT」。

識別符：VPC_PEERING_DNS_RESOLUTION_CHECK

資源類型:AWS:: EC2:: VPC PeeringConnection

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

vpcIds (選用), 類型：CSV

要檢查的 VPC ID 清單 (以逗號分隔)。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## vpc-sg-open-only-to-authorized-ports

檢查安全群組是否允許不受限制的傳入流量 ('0.0.0.0/0' 或 '::/0') 只允許授權連接埠上的傳入 TCP 或 UDP 連線。如果此類安全群組沒有在規則參數中指定的連接埠，則表示規則為「NON_COMPLIANT」。

> **Note**
>
> 此規則會評估輸入規則設定為 IPv4='0.0.0.0/0' 或 IPv6='::/' 的 Amazon EC2 安全群組。如果安全群組沒有其中一個目的地，則此規則會傳回 `NOT_APPLICABLE`。

識別符 : VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

資源類型： AWS::EC2::SecurityGroup

觸發類型： Configuration changes (組態變更) 和 Periodic (定期)。

AWS 區域：所有支援的 AWS 地區

參數：

authorizedTcpPorts (選擇性), 類型：字串

以逗號分隔的 TCP 連接埠清單，已授權開放給 0.0.0.0/0 或 ::/0。範圍以破折號定義，例如「443,1020-1025」。

authorizedUdpPorts (選擇性), 類型：字串

以逗號分隔的 UDP 連接埠清單，已授權開放給 0.0.0.0/0 或 ::/0。範圍以破折號定義，例如「500,1020-1025」。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## VPC-NG 端口限制檢查

檢查安全群組是否將傳入流量明確限制在 0.0.0.0/0 或:/0 之間的限制連接埠。如果安全群組允許透過 TCP/UDP 連接埠 22/3389 從 0.0.0/0 或:: /0 傳入流量，或如參數中所指定，則該規則為「不相容」。

識別碼：VPC_SG_ 端口 _ 限制 _ 檢查

資源類型： AWS::EC2::SecurityGroup

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

限制連接埠 (選用), 類型：CSV

不應針對完整 IP 範圍內的傳入流量開啟的連接埠清單 (以逗號分隔)。有效的通訊埠號碼範圍介於 0 到 65535 之間。如果未指定，則規則預設為檢查 22 和 3389。

通訊協定型態 (選擇性), 類型：字串

要檢查之規則的「傳輸通訊協定類型」。有效值包括「TCP」、「UDP」和「全部」(不區分大小寫)。如果設定為「ALL」，則規則會檢查使用「TCP」、「UDP」或「全部」(-1) 通訊協定的規則。默認值為「全部」。

排除ExternalSecurityGroups（可選），類型：布林值

用於排除外部安全性群組評估的布林旗標。如果設定為 'true'，則規則將不會在評估中包含外部安全性群組。否則，如果值設定為「false」，則會評估所有安全性群組。默認值是 '真'。

IP 類型 (選擇性), 類型：字串

要檢查之規則的網際網路通訊協定 (IP) 版本。有效值包括「IPv4」、「IPv6」和「全部」(不區分大小寫)。如果未指定，則規則預設會檢查「全部」。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## vpc-vpn-2-tunnels-up

檢查 AWS 站台對站 VPN 提供的兩個虛擬私人網路 (VPN) 通道是否處於啟動狀態。如果其中一或兩個通道都處於 DOWN (關閉) 狀態，則表示規則為「NON_COMPLIANT」。

識別符： VPC_VPN_2_TUNNELS_UP

資源類型：AWS::EC2::VPNConnection

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## wafv2-logging-enabled

檢查 AWS WAFv2 地區和全球 Web 存取控制清單 (Web ACL) 上是否已啟用記錄。如果已啟用日誌記錄，但日誌記錄目的地與參數值不相符，則表示規則為「NON_COMPLIANT」。

識別符： WAFV2_LOGGING_ENABLED

資源類型 AWS::WAFv2::Web:

觸發類型：定期

AWS 區域：所有支援的 AWS 地區

參數：

KinesisFirehoseDeliveryStreamArns (選擇性), 類型：CSV

Kinesis Firehose 交付串流 ARN 的清單 (以逗號分隔)

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## wafv2-rulegroup-logging-enabled

檢查 AWS WAFv2 規則群組上的 Amazon CloudWatch 安全指標收集是否已啟用。如果是 '，則該規則是「不符合 _」。VisibilityConfig CloudWatchMetricsEnabled'欄位設定為假。

內容： AWS WAFV2 （Web 應用程式防火牆第 2 版）可讓您建立 AWS WAF 規則，以保護您的 Web 應用程式不受常見 Web 入侵和弱點的侵害。規 AWS WAF 則群組是一組 AWS WAF 規則，您可以與 Web ACL (存取控制清單) 產生關聯，以定義 Web 應用程式流量所需的行為。如需詳細資訊，請參閱AWS WAF 開發人員指南中的AWS WAF 規則和規則群組。

透過在 AWS WAFV2 規則群組上設定 CloudWatch 安全指標收集，您可以監視安全指標，例如成功或失敗的分散式拒絕服務 (DDoS)、SQL 插入和跨網站指令碼 (XSS) 攻擊。收集到的安全指標可以幫助您簡化調查。

> **Note**
> 如果要檢查受管理 AWS WAF 規則的規 AWS WAFV2 則群組中沒有規則，則 AWS Config 受管 AWS Config 理規則會傳回 NON_APPLY。

識別符：WAFV2_RULEGROUP_LOGGING_ENABLED

資源類型： AWS::WAFv2::RuleGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## wafv2-rulegroup-not-empty

檢查 WAFv2 規則群組是否包含規則。如果 WAFv2 規則群組中沒有規則，則表示規則為「NON_COMPLIANT」。

識別符：WAFV2_RULEGROUP_NOT_EMPTY

資源類型： AWS::WAFv2::RuleGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## wafv2-webacl-not-empty

檢查 WAFv2 Web ACL 是否包含任何 WAF 規則或 WAF 規則群組。如果 Web ACL 不包含任何 WAF 規則或 WAF 規則群組，則表示此規則為「NON_COMPLIANT」。

識別符：WAFV2_WEBACL_NOT_EMPTY

資源類型 AWS::WAFv2::Web:

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## waf-classic-logging-enabled

檢查 AWS WAF 傳統全域 Web 存取控制清單 (Web ACL) 上是否已啟用記錄。如果全域 Web ACL 沒有啟用日誌記錄，則表示規則為「NON_COMPLIANT」。

識別符：WAF_CLASSIC_LOGGING_ENABLED

資源類型 AWS::WAF::Web:

觸發類型：定期

AWS 區域：僅在美國東部 (維吉尼亞北部) 區域提供

參數：

KinesisFirehoseDeliveryStreamArns (選擇性), 類型：CSV

以逗號分隔的 Amazon Kinesis 串流 ARN 清單，適用於 AWS WAF 日誌。

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## waf-global-rulegroup-not-empty

檢查 AWS WAF 典型規則群組是否包含任何規則。如果規則群組中沒有規則，則表示規則為「NON_COMPLIANT」。

識別符：WAF_GLOBAL_RULEGROUP_NOT_EMPTY

資源類型： AWS::WAF::RuleGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## waf-global-rule-not-empty

檢查 AWS WAF 全域規則是否包含任何條件。如果 WAF 全域規則內沒有任何條件，則表示規則為「NON_COMPLIANT」。

識別符：WAF_GLOBAL_RULE_NOT_EMPTY

資源類型： AWS::WAF::Rule

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## waf-global-webacl-not-empty

檢查 WAF 全域 Web ACL 是否包含任何 WAF 規則或規則群組。如果 Web ACL 不包含任何 WAF 規則或規則群組，則表示此規則為「NON_COMPLIANT」。

識別符：WAF_GLOBAL_WEBACL_NOT_EMPTY

資源類型 AWS::WAF::Web:

觸發類型： Configuration changes (組態變更)

AWS 區域：只有在美國東部 (維吉尼亞北部) 區域提供

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## waf-regional-rulegroup-not-empty

檢查 WAF 區域規則群組是否包含任何規則。如果 WAF 區域規則群組中沒有規則，則表示規則為「NON_COMPLIANT」。

識別符：WAF_REGIONAL_RULEGROUP_NOT_EMPTY

資源類型： AWS::WAFRegional::RuleGroup

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## waf-regional-rule-not-empty

檢查 WAF 區域規則是否包含條件。如果地區規則至少包含一個條件，則表示此規則為「COMPLIANT」，否則為「NON_COMPLIANT」。

識別符：WAF_REGIONAL_RULE_NOT_EMPTY

資源類型： AWS::WAFRegional::Rule

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

### waf-regional-webacl-not-empty

檢查 WAF 區域 Web ACL 是否包含任何 WAF 規則或規則群組。如果 Web ACL 中沒有 WAF 規則或規則群組，則表示規則為「NON_COMPLIANT」。

識別符：WAF_REGIONAL_WEBACL_NOT_EMPTY

資源類型 AWS::WAFRegional::Web:

觸發類型： Configuration changes (組態變更)

AWS 區域：所有支援的 AWS 地區

參數：

無

AWS CloudFormation 範本

若要使用 AWS CloudFormation 範本建立 AWS Config 受管規則，請參閱建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。

## 按評估模式排序的 AWS Config 受管理規則清單

AWS Config 目前支援下列受管規則。

### 考量事項

受管規則的預設值

只有在使用 AWS 主控台時，才會預先填入針對受管理規則指定的預設值。不提供 API、CLI 或 SDK 的預設值。

不支援目錄值區

受管規則僅在評估 Amazon 簡單儲存服務 (Amazon S3) 資源時支援一般用途儲存貯體。 AWS Config 不會記錄目錄值區的組態變更。如需一般用途儲存貯體和目錄儲存貯體的詳細資訊，請參閱 Amazon S3 使用者指南中的儲存貯體概觀和目錄儲存貯體。

受管規則和全域 IAM 資源類型

2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022 年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。

為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

## 主動評估

主動規則是支援尚未部署資源之主動評估模式的規則。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是「非符合」(NON_COMPLUTION)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。 AWS 如需詳細資訊，請參閱《評估模式》。

> **Note**
>
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

主動評估

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check

- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-check
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled

## 偵測評估

偵測規則是支援已部署資源之偵測評估模式的規則。這可讓您評估現有資源的組態設定。

> **Note**
>
> 目前，所有 AWS Config 規則都支持偵探評估。

### 偵測評估

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled

- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用

- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check

- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled

- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-S3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-服務器證書過期檢查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 按觸發類型排序的 AWS Config 受管理規則清單

AWS Config 目前支援下列受管規則。

### 考量事項

受管規則的預設值

只有在使用 AWS 主控台時，才會預先填入針對受管理規則指定的預設值。不提供 API、CLI 或 SDK 的預設值。

不支援目錄值區

受管規則僅在評估 Amazon 簡單儲存服務 (Amazon S3) 資源時支援一般用途儲存貯體。 AWS Config 不會記錄目錄值區的組態變更。如需一般用途儲存貯體和目錄儲存貯體的詳細資訊，請參閱 Amazon S3 使用者指南中的儲存貯體概觀和目錄儲存貯體。

受管規則和全域 IAM 資源類型

2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022

年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。

為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。如需哪些區域支援受管理規則的清單，請參閱依區域可用性區域排列的 AWS Config 受管規則清單。

## 組態變更

變更觸發的規則是為了回應組態變更而進行 AWS Config 評估的規則。

組態變更

- acm-certificate-rsa-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-client-vpn-connection-log-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- global-endpoint-event-replication-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check

- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-雲觀察審計日誌啟用
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication

- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- 與組織內共用的服務目錄
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty

- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 定期

週期性規則是按照您指定的頻率進行定期 AWS Config 評估的規則，例如，每 24 小時一次。

定期

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan

- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks-群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用

- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-S3 保護啟用
- 啟用 Iam 外部存取分析器
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-服務器證書過期檢查
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- 中國火花交付流加密
- kms-cmk-not-scheduled-for-deletion
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled
- rds-in-backup-plan
- rds-last-backup-recovery-point-created

- rds-meets-restore-time-target
- rds-resources-protected-by-backup-plan
- 無限制的紅移連接埠存取
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-flow-logs-enabled
- VPC-NG 端口限制檢查
- wafv2-logging-enabled

- waf-classic-logging-enabled

### 混合

混合規則是針對組態變更和定期進行 AWS Config 評估的規則。

混合

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- incoming-ssh-disabled
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

## 按區域可用性分類的 AWS Config 受管規則清單

AWS Config 目前支援下列受管規則。

### 考量事項

受管規則的預設值

只有在使用 AWS 主控台時，才會預先填入針對受管理規則指定的預設值。不提供 API、CLI 或 SDK 的預設值。

不支援目錄值區

受管規則僅在評估 Amazon 簡單儲存服務 (Amazon S3) 資源時支援一般用途儲存貯體。 AWS Config 不會記錄目錄值區的組態變更。如需一般用途儲存貯體和目錄儲存貯體的詳細資訊，請參閱 Amazon S3 使用者指南中的儲存貯體概觀和目錄儲存貯體。

受管規則和全域 IAM 資源類型

2022 年 2 月之前登入的全球 IAM 資源類型 (`AWS::IAM::Group`、`AWS::IAM::PolicyAWS::IAM::Role`、和`AWS::IAM::User`) 只能在 2022

年 2 月之前提供的 AWS 區域 AWS Config 中 AWS Config 記錄。這些資源類型無法在 2022 年 2 月 AWS Config 之後支援的地區中記錄。如需這些區域的清單，請參閱錄製 AWS 資源 | 全域資源。

如果您至少在一個區域中記錄全域 IAM 資源類型，則針對全域 IAM 資源類型報告合規的週期性規則將會在新增週期性規則的所有區域執行評估，即使您尚未在新增週期性規則的區域中啟用全域 IAM 資源類型的記錄也是如此。

為了避免不必要的評估，您應該只將報告全域 IAM 資源類型合規的定期規則部署到其中一個支援的區域。

## 美國東部 (俄亥俄) 區域

美國東部 (俄亥俄)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用

- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled

- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 美國東部 (維吉尼亞北部) 區域

### 美國東部 (維吉尼亞北部)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag

- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured

- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted

- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created

- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target

- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-服務器證書過期檢查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查

- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄

- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty

- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 美國西部 (加利佛尼亞北部) 區域

### 美國西部 (加利佛尼亞北部)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護

- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 美國西部 (奧勒岡) 區域

### 美國西部 (奧勒岡)

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check

- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings

- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 非洲 (開普敦) 區域

### 非洲 (開普敦)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted

- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- 啟用 DMS-雷迪斯
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user

- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled

- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-雲觀察審計日誌啟用
- mq-rabbit-deployment-mode

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest

- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 亞太區域 (香港) 區域

### 亞太區域 (香港)

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit

- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan

- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 亞太區域 (海德拉巴)

### 亞太區域 (海德拉巴)

- acm-certificate-expiration-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs 掛載目標-公共可訪問
- eip-attached
- eks-cluster-log-enabled
- eks-群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only

- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 安全防護-s3 保護啟用
- 啟用 Iam 外部存取分析器
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- 中國火花交付流加密
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-default-admin-check
- redshift-default-db-name-check
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check

- 命形器-端點配置-配置-實例計數
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

## 亞太區域 (雅加達)

### 亞太區域 (雅加達)

- access-keys-rotated
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-multiple-az
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled

- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs 掛載目標-公共可訪問
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version

- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- 中國火花交付流加密
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-雲觀察審計日誌啟用
- mq-rabbit-deployment-mode
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-default-admin-check
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

## 亞太區域 (墨爾本) 區域

### 亞太區域 (墨爾本)

- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查

- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs 掛載目標-公共可訪問
- eip-attached
- eks-群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 安全防護-s3 保護啟用
- 啟用 Iam 外部存取分析器
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 亞太 (孟買) 區域

### 亞太區域 (孟買)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest

- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用

- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用

- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

## 亞太 (大阪) 區域

### 亞太區域 (大阪)

- access-keys-rotated
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查

- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-table-deletion-protection-enabled

- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-launch-template-public-ip-disabled
- ec2-no-amazon-key-pair
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecs-containers-readonly-access
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs 掛載目標-公共可訪問
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elbv2-multiple-az
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-function-public-access-prohibited
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-cluster-default-admin-check
- rds-cluster-encrypted-at-rest
- rds-instance-default-admin-check
- rds-instance-public-access-check
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 與組織內共用的服務目錄
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-peering-dns-resolution-check
- VPC-NG 端口限制檢查
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 亞太 (首爾) 區域

### 亞太區域 (首爾)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest

- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit

- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized

- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 亞太 (新加坡) 區域

### 亞太區域 (新加坡)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled

- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging

- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit

- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized

- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty

- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 亞太 (雪梨) 區域

### 亞太區域 (悉尼)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用

- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 亞太 (東京) 區域

### 亞太區域 (東京)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證

- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 加拿大 (中部) 區域

### 加拿大 (中部)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證

- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check

- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled

- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用安全防護惡意軟體保護
- guardduty-non-archived-findings
- 啟用防護-RDS 保護
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 加拿大西部 (卡加利) 區域

### 加拿大西部 (卡加利)

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- approved-amis-by-id
- approved-amis-by-tag
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- eip-attached
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

## 中國 (北京) 區域

### 中國 (北京)

- access-keys-rotated
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan

- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check

- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access

- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 中國 (寧夏) 區域

### 中國 (寧夏)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan

- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check

- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 歐洲 (法蘭克福) 區域

### 歐洲 (法蘭克福)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted

- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created

- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target

- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check

- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw

- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled

- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 歐洲 (愛爾蘭) 區域

### 歐洲 (愛爾蘭)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check

- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check

- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查

- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 歐洲 (倫敦) 區域

### 歐洲 (倫敦)

- access-keys-rotated
- account-part-of-organizations

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit

- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption

- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted

- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions

- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target

- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Europe (Milan) Region

### 歐洲 (米蘭)

- access-keys-rotated
- account-part-of-organizations

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- 啟用 DMS-雷迪斯
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- 無限制的紅移連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 歐洲 (巴黎) 區域

Europe (Paris)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni

- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-version
- eks-群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 歐洲 (西班牙) 區域

### 歐洲 (西班牙)

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs 掛載目標-公共可訪問
- eip-attached
- eks-cluster-log-enabled
- eks 群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 安全防護-s3 保護啟用
- 啟用 Iam 外部存取分析器
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- 中國火花交付流加密
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- rds-instance-default-admin-check
- redshift-default-admin-check
- redshift-default-db-name-check
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

## 歐洲 (斯德哥爾摩) 區域

### 歐洲 (斯德哥爾摩)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted

- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled

- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks 群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查器羔羊代碼掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target

- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 歐洲 (蘇黎世) 區域

### 歐洲 (蘇黎世)

- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs 掛載目標-公共可訪問
- eip-attached
- eks-cluster-log-enabled
- eks 群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- elb-deletion-protection-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 安全防護-s3 保護啟用
- 啟用 Iam 外部存取分析器
- iam-password-policy
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-snapshot-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled

- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

## 以色列 (特拉維夫) 區域

### 以色列 (特拉維夫)

- account-part-of-organizations
- alb-desync-mode-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az

- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- 安全防護-s3 保護啟用
- incoming-ssh-disabled

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- Macie-自動敏感的數據發現檢查
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic

- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-network-acl-unused-check

- VPC-NG 端口限制檢查
- wafv2-webacl-not-empty

## Middle East (Bahrain) Region

### Middle East (Bahrain)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-version
- eks 群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check

- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured

- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## 中東 (阿拉伯聯合大公國) 區域

### 中東 (阿拉伯聯合大公國)

- account-part-of-organizations
- acm-certificate-expiration-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查

- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs 掛載目標-公共可訪問
- eks-cluster-log-enabled
- eks 群集秘密加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access

- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 安全防護-s3 保護啟用
- 啟用 Iam 外部存取分析器
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-雲觀察審計日誌啟用
- mq-rabbit-deployment-mode

- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- 命形器-端點配置-配置-實例計數
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- ssm-document-not-public

- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

## 南美洲 (聖保羅) 區域

### 南美洲 (聖保羅)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id

- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- Dax-tls 端點加密
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks 群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check

- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 警衛-EK-保護審計啟用
- 防護-EK 保護-運行時啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- 啟用防護惡意軟體保護功能
- guardduty-non-archived-findings
- 啟用防護-RDS 保護功能
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- 啟用 Iam 外部存取分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用

- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- Macie-自動敏感的數據發現檢查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-雲觀察審計日誌啟用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-db-security-group-not-allowed

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## AWS GovCloud (美國東部) 區域

### AWS GovCloud (美國東部)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks 群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check

- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-resources-protected-by-backup-plan
- 警衛-EK-保護審計啟用
- guardduty-enabled-centralized
- 啟用了防守羔羊保護
- guardduty-non-archived-findings
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check

- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-雲觀察審計日誌啟用
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- 與組織內共用的服務目錄

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## AWS GovCloud (美國西部) 區域

### AWS GovCloud (美國西部)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- 雲徑-全讀-S3-數據事件檢查
- 雲跟踪全寫 S3 數據事件檢查
- 雲通道 S3-桶訪問日誌
- 雲路-s3 桶公共訪問禁止
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- 啟用 DMS-蒙古 DB-身份驗證
- DMS-海王星 IAM 授權啟用
- 啟用 DMS-雷迪斯
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs 掛載目標-公共可訪問
- efs-resources-protected-by-backup-plan
- eip-attached
- eks 群集秘密加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-resources-protected-by-backup-plan
- 警衛-EK-保護審計啟用
- guardduty-enabled-centralized

- 啟用了防守羔羊保護
- guardduty-non-archived-findings
- 安全防護-s3 保護啟用
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-服務器證書過期檢查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 檢查器-ec2-掃描啟用
- 檢查器 ECR-掃描啟用
- 檢查員-羔羊標準掃描啟用
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- 中國火花交付流加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-雲觀察審計日誌啟用
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- 打開搜索主要節點容錯
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- 未受限制的無限制連接埠存取
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 啟用 S3 儲存區跨區域複寫
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created

- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- 命形器-端點配置-配置-實例計數
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- 與組織內共用的服務目錄
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 傳輸家庭服務器-無 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- VPC-NG 端口限制檢查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## 服務連結規 AWS Config 則

服務連結規 AWS Config 則是一種獨特的 AWS Config 受管規則類型，可支援其他 AWS 服務在您的帳戶中建立 AWS Config 規則。服務連結規則已預先定義為包含代表您呼叫其他 AWS 服務所需的所有權限。這些規則與 AWS 服務針對合規性驗證所建議 AWS 帳戶 的標準類似。

這些服務連結 AWS Config 規則由 AWS 服務團隊擁有。服 AWS 務團隊會在您的 AWS 帳戶. 您只能唯讀存取這些規則。如果您訂閱了這些規則所連結的 AWS 服務，則無法編輯或刪除這些規則。

服務連結規則及 AWS Command Line Interface

使用PutConfig規則 AWS CLI、DeleteConfig規則和DeleteEvaluation結果 API 傳回拒絕存取，並顯示下列錯誤訊息：

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

服務連結規則和主 AWS Config 控台

在 AWS Config 主控台中，服務連結 AWS Config 規則會顯示在「規則」頁面中。主控台中的 [編輯] 和 [刪除結果] 按鈕會呈現灰色，限制您無法編輯規則。您可以藉由選擇規則來檢視規則的詳細資訊。

服務連結規則、補救動作和一致性套件

若要將修正動作新增至符合性套件中的服務連結規則，您需要將修正動作新增至一致性套件範本本身，然後使用更新的範本更新一致性套件。如需有關更新一致性套件的資訊，請參閱部署一致性套件 (主控台)、部署一致性套件 (AWS CLI) 和管理組織一致性套件。

編輯和刪除服務連結規則

若要編輯或刪除服務連結規則，請連絡建立規則的 AWS 服務。例如，針對由建立的服務連結規則 AWS Security Hub，您可以依照使用AWS Security Hub 者指南中的下列步驟移除服務連結規則：停用安全性標準。

## 建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)

> **Important**
>
> 您必須先建立並啟動AWS Config組態錄製程式，才能使用建立AWS Config受管規則AWS CloudFormation。如需詳細資訊，請參閱管理組態記錄器。

針對支援的 AWS Config 受管規則，您可以使用 AWS CloudFormation 範本來建立帳戶的規則，或是更新現有的 AWS CloudFormation 堆疊。堆疊是您佈建並更新為單一單位相關資源的集合。當您使用範本啟動堆疊時，系統即會為您建立 AWS Config 受管規則。範本僅會建立規則，而不建立其他 AWS 資源。

> **Note**
>
> 更新 AWS Config 受管規則時，範本也會更新為含最新的變更。若要儲存規則的特定範本版本，請下載範本，並將其上傳至您的 S3 儲存貯體。

若要取得有關使用AWS CloudFormation範本的更多資訊，請參閱《AWS CloudFormation使用指南》AWS CloudFormation中的〈入門〉。

啟動 AWS CloudFormation 堆疊 (AWS Config 受管規則)

1. 轉到CloudFormation控制台並創建一個新的堆棧。
2. 針對 Specify template (指定範本)：
   - 若您下載範本，請選擇 Upload a template (上傳範本)，然後選擇檔案以上傳範本。
   - 您也可以選擇 Amazon S3 網址，然後輸入範本網址`http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/`*`THE_RULE_IDENTIFIER`*`.template`。

   > **Note**
   >
   > 規則識別碼應使用具有 _ 底線的所有 _CAPS_ 撰寫。例如，雲觀察 _ 日誌組 _ 加密而不是 cloudwatch-log-group-encrypted.
   > 對於某些規則，規則識別碼與規則名稱不同。確保使用編選項。例如，受限制的 ssh 的規則識別碼為「連入 _ SSH_ 已停用」。

3. 選擇 Next (下一步)。
4. 針對 Specify stack details (指定堆疊詳細資訊)，輸入堆疊名稱並輸入 AWS Config 規則的參數值。例如，若您使用 `DESIRED_INSTANCE_TYPE` 受管規則範本，您可以指定執行個體類型 (像是 "m4.large")。
5. 選擇 Next (下一步)。
6. 您可針對 Options (選項) 建立標籤，或設定其他進階選項。這些並非必要項目。

7. 選擇 Next (下一步)。
8. 針對 Review (檢閱)，確認範本、參數及其他選項皆正確。
9. 選擇 Create (建立)。堆疊幾分鐘內就能建立。您可以在 AWS Config 主控台 中檢視建立的規則。

您可以使用範本建立 AWS Config 受管規則的單一堆疊，或是更新您帳戶中的現有堆疊。若您刪除堆疊，從該堆疊建立的受管規則也會刪除。如需詳細資訊，請參閱《使用指南》中的〈AWS CloudFormation使用堆疊〉。

# AWS Config 自訂規則

AWS Config 自訂規則是您從頭開始建立的規則。建立 AWS Config 自訂規則的方法有兩種：使用 Lambda 函數 (AWS Lambda 開發人員指南)，以及使用 Guard (安全防護 GitHub儲存庫) (一種 policy-as-code 語言)。

AWS Config 使用 Lambda 建立的自訂規則稱為AWS Config 自訂 Lambda 規則，而 AWS Config 使用防護建立的自訂規則稱為AWS Config 自訂原則規則。

## AWS Config 自訂原則規則

使用安全警衛撰寫的規則可以從 AWS Config 主控台或使用 AWS Config 規則 API 建立。 AWS Config 自訂原則規則可讓您建立 AWS Config 自訂規則，而不需要使用 Java 或 Python 來開發 Lambda 函數來管理您的自訂規則。 AWS Config 自訂原則規則是由組態變更所啟動。如需有關安全警衛的詳細資訊，請參閱守門員 GitHub儲存庫

## AWS Config 自訂 Lambda 規則

自訂 Lambda 規則可讓您選擇使用 Java 或 Python 為 AWS Config 自訂規則建立 Lambda 函數。Lambda 函數是您上傳的自訂程式碼 AWS Lambda，而且會由事件來源發佈至該函數的事件叫用。如果 Lambda 函數與規則相關聯， AWS Config 則會在規則啟動時 AWS Config 呼叫該函數。然後，Lambda 函數會評估傳送的組態資訊 AWS Config，並傳回評估結果。如需 Lambda 函數的詳細資訊，請參閱《AWS Lambda 開發人員指南》中的函數和事件來源一節。

## 成本考量

如需與資源記錄相關聯的成本詳細資訊，請參閱AWS Config 定價。

建議：新增邏輯以處理自訂 lambda 規則的已刪除資源評估

建立 AWS Config 自訂 lambda 規則時，強烈建議您新增邏輯來處理已刪除資源的評估。

當評估結果標記為 NOT_APPLICABLE 時，其會被標記以進行刪除和清理。如果評估結果未標記為 NOT_APPLICABLE，則直到刪除規則為止，其將保持不變，這可能會導致在刪除規則時，意外大量建立 AWS::Config::ResourceCompliance 的組態項目 (CI)。

如需如何設 AWS Config 定自訂 lambda 規則以傳回已刪除資源的相NOT_APPLICABLE關資訊，請參閱使用 AWS Config 自訂 lambda 規則管理已刪除的資源。

建議：提供自訂 lambda 規則範圍內的資源

AWS Config 如果規則的範圍不限於一或多個資源類型，則自訂 Lambda 規則可能會導致大量 Lambda 函數叫用。為了避免與您的帳戶相關聯的活動增加，強烈建議您為自訂 Lambda 規則提供範圍內的資源。如果未選取任何資源類型，則規則會針對帳戶中的所有資源叫用 Lambda 函數。

建議：在刪除規則之前停止記錄資源符合性

強烈建議您在刪除帳戶中的規則之前停止記錄AWS::Config::ResourceCompliance資源類型。刪除規則會建立 CI，AWS::Config::ResourceCompliance且可能會影響您的 AWS Config 組態記錄器成本。如果您要刪除評估大量資源類型的規則，這可能會導致記錄的 CI 數量激增。

最佳做法：

1. 停止錄製 AWS::Config::ResourceCompliance
2. 刪除規則
3. 開啟錄影功能 AWS::Config::ResourceCompliance

## 觸發類型

將規則新增至帳戶後，請 AWS Config 將資源與規則條件進行比較。在此初始評估之後，每次觸發評估時都會 AWS Config 繼續執行評估。評估觸發程序被定義為規則的一部分，它們可以包括下列類型。

| 觸發類型 | Description |
| --- | --- |
| 組態變更 | AWS Config 當有符合規則範圍的資源，且資源的組態發生變更時，會執行規則的評估。評估會在 AWS Config 傳送組態項目變更通知後執行。<br><br>您可以透過定義規則的範圍來選擇要進行評估的資源。範圍可包含下列項目： |

| 觸發類型 | Description |
| --- | --- |
| | • 一或多個資源類型<br>• 資源類型和資源 ID 的組合<br>• 標籤鍵和值的組合<br>• 當任何記錄的資源建立、更新或刪除時<br><br>AWS Config 當偵測到符合規則範圍的資源變更時，會執行評估。您可以使用範圍來定義要進行評估的資源。 |
| 定期 | AWS Config 以您選擇的頻率執行規則的評估，例如，每 24 小時執行一次。 |
| 混合 | 部分規則同時具有組態變更和定期觸發條件。對於這些規則，請在偵測到組態變更時以及您指定的頻率 AWS Config 評估您的資源。 |

## 評估模式

AWS Config 規則有兩種評估模式。

| 評估模式 | Description |
| --- | --- |
| 主動 | 使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是 AWS 「非符合」(NON_COMPLIGENTING)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。<br><br>如需詳細資訊，請參閱《評估模式》。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。 |
| 偵測 | 使用偵測評估來評估已部署的資源。這可讓您評估現有資源的組態設定。 |

> **Note**
>
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

## 使用 AWS Config 自訂 lambda 規則管理已刪除的資源

報告已刪除資源的規則，應傳回的 `NOT_APPLICABLE` 評估結果，以避免不必要的規則評估。

當您刪除資源時， AWS Config `configurationItem`會`ResourceDeleted`建立`configurationItemStatus`. 您可以使用此中繼資料來檢查規則是否報告已刪除的資源。如需組態項目的詳細資訊，請參閱《概念 | 組態項目》。

包含下列程式碼片段以檢查已刪除的資源，並將 AWS Config 自訂 lambda 規則的評估結果設定為`NOT_APPLICABLE`如果報告已刪除的資源：

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
```

```
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config 受管規則和 AWS Config 自訂原則規則預設會處理此行為。
> 如果您使用開發工具包（RDK）和 AWS Config AWS Config 開發工具包庫（RDK）使用 Python 創建 AWS Config 自定義 lambda 規則，則導入的評估器類將檢查此行為。如需如何使用 RDK 和 RDKLib 撰寫規則的相關資訊，請參閱《使用 RDK 和 RDKLib 撰寫規則》。

主題


- 建立 AWS Config 自訂原則規則
- 正在建立AWS ConfigLambda 訂


## 建立 AWS Config 自訂原則規則

您可以從 AWS Management Console、 AWS CLI或 AWS Config API 建立 AWS Config 自訂原則規則。如需有關如何使用安全警衛撰寫規則的詳細資訊，請參閱守門員使用指南中的撰寫 AWS CloudFormation 守門員規則。如需有關 AWS Config 可評估之受支援資源類型結構描述的詳細資訊，請參閱資源結構描述 GitHub 儲存庫中的 AWS Config 資源類型。

> **Important**
>
> 用來評估組態項目的 AWS Config 資源結構描述與用來評估 AWS CloudFormation 範本的 CFN 結構描述不同。如果您將 CFN 結構描述用於 AWS Config 自訂政策規則，則會傳回 `NOT_APPLICABLE` 評估結果。建立 AWS Config 自訂原則規則並根據組態項目結構寫入策略時，請使用 AWS Config 資源結構描述。如需 AWS Config 資源結構描述的清單，請參閱資源結構描述 GitHub 儲存庫中的 AWS Config 資源類型。

### 建立 AWS Config 自訂原則規則 (主控台)

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。

2. 在 AWS Management Console 功能表中，確認 [地區] 選取器已設定為支援 AWS Config 規則的 [ AWS 地區]。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在左側導覽中，選擇 規則。
4. 在 Rules (規則) 頁面，選擇 Add rule (新增規則)。
5. 在 指定規則類型 頁面上，請選擇 使用 Guard 建立自訂規則。
6. 在 設定規則 頁面上，請完成下列步驟以建立規則：

   a. 針對 規則名稱，請鍵入規則的唯一名稱。
   b. 針對 描述，請鍵入規則的描述。
   c. 針對「安全警衛」執行階段版本，選擇 AWS Config 自訂原則規則的執行階段系統。
   d. 針對 規則內容，您可以為規則填入 Guard 自訂政策。如需有關防護自訂原則之結構和功能的詳細資訊，請參閱AWS CloudFormation 安全防護 GitHub 儲存庫中的安全防護 2.0 的作業模式。

   > **Note**
   > 用來評估組態項目的 AWS Config 資源結構描述與用來評估 AWS CloudFormation 範本的 CFN 結構描述不同。如果您將 CFN 結構描述用於 AWS Config 自訂政策規則，則會傳回 `NOT_APPLICABLE` 評估結果。建立 AWS Config 自訂原則規則並根據組態項目結構寫入策略時，請使用 AWS Config 資源結構描述。如需清單 AWS Config 資源結構描述，請參閱資源結構描述 GitHub 儲存庫中的 AWS Config 資源類型。

   下列範例顯示受 AWS Config 管理規則之 AWS Config 自訂原則規則版本的原則定義 dynamodb-pitr-enabled

```
# This rule checks if point in time recovery (PITR) is enabled on active Amazon
 DynamoDB tables
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
```

```
    tableisactive {
        let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription
        %pitr == "ENABLED"
}
```

e. AWS Config 若為「評估」模式，請選擇您要在資源建立與管理程序中評估資源的時間。根據規則， AWS Config 可以在佈建資源之前、提供資源之後或兩者之後評估您的資源組態。

   i. 選擇 開啟主動評估，可讓您在部署資源之前，對資源的組態設定執行評估。

      啟用主動式評估之後，您可以使用StartResource評估 API 和 GetResourceEvaluationSummaryAPI 來檢查您在這些命令中指定的資源是否會被您所在地區帳戶中的主動規則標記為「NON_COMPLUTION」。

      如需有關使用此命令的詳細資訊，請參閱使用 AWS Config 規則評估資源。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。

   ii. 選擇 開啟偵測評估 以評估現有資源的組態設定。

      針對偵測評估， AWS Config 自訂原則規則會由組態變更啟動。此選項將被預先選擇。

      - 資源 – 建立、變更或刪除符合指定資源類型或加上識別符類型的資源時。
      - 標籤 – 建立、變更或刪除含指定標籤的資源時。
      - 所有變更 — 建立、變更或刪除記錄的資源時。 AWS Config

      AWS Config 當偵測到符合規則範圍的資源變更時，會執行評估。您可以使用範圍來限制要進行評估的資源。否則，當佈建後的資源發生變更時，會啟動評估。

f. 針對 參數，如果您的規則包含參數，則您可以自訂所提供金鑰的值。您的資源必須依循參數這項屬性，才會被視為符合規則。

7. 在 [檢閱並建立] 頁面上，檢閱所有選取項目，然後再將規則新增至您的 AWS 帳戶。
8. 檢閱完規則後，請選擇 新增規則。

## 建立 AWS Config 自訂原則規則 (AWS CLI)

使用 `put-config-rule` 命令。

該 `Owner` 欄位應為 `CUSTOM_POLICY`。 AWS Config 自訂原則規則需要下列其他欄位：

- `Runtime`： AWS Config 自訂原則規則的執行階段系統。
- `PolicyText`：包含 AWS Config 自訂政策規則邏輯的政策定義。
- `EnableDebugLogDelivery`：啟用 AWS Config 自訂原則規則偵錯記錄的布林運算式。預設值為 `false`。

### 建立 AWS Config 自訂原則規則 (API)

使用「PutConfig規則」動作。

該 `Owner` 欄位應為 `CUSTOM_POLICY`。 AWS Config 自訂原則規則需要下列其他欄位：

- `Runtime`： AWS Config 自訂原則規則的執行階段系統。
- `PolicyText`：定義 AWS Config 自訂政策規則邏輯的政策。
- `EnableDebugLogDelivery`：啟用 AWS Config 自訂原則規則偵錯記錄的布林運算式。預設值為 `false`。

## 正在建立AWS ConfigLambda 訂

您可以開發自訂規則並將其新增至AWS Config取代為AWS Lambda函數。您可以將每個自訂規則與 Lambda 函數產生關聯，該函數包含評估是否您的AWS資源符合規則。您將此函數與您的規則建立關聯，規則便會在回應組態變更時或定期呼叫函數。函數接著便會評估您的資源是否符合您的規則，並將評估結果傳送到 AWS Config。

範例自訂 Lambda 規則 (Amazon EC2 範例)引導您首次建立自訂 Lambda 規則，以評估每個 EC2 執行個體是否為 t2.micro 類型。其中包含可 Lambda 於您可以新增至AWS Lambda沒有修改。範例自訂 Lambda 規則 (一般範例)提供建立自訂 Lambda 規則的更一般範例。

若要了解如何操作AWS Lambda功能工作以及如何開發它們，請參閱AWS Lambda開發人員指南。

主題


- 自訂 Lambda 規則 (Amazon EC2 範例)
- 自訂 Lambda 規則 (一般範例)
- AWS Config 規則的範例 AWS Lambda 函數和事件

## 自訂 Lambda 規則 (Amazon EC2 範例)

此程序會引導您完成建立自訂 Lambda 規則的程序，以評估每個 EC2 執行個體是否為 t2.micro 類型。AWS Config 將針對此規則執行基於事件的評估，這表示每次 AWS Config 偵測到執行個體中的組態變更時，它都會檢查您的執行個體設定。 AWS Config 會將 t2.micro 執行個體標記為相容，並將所有其他執行個體標記為不相容。合規狀態會顯示在 AWS Config 主控台。

為了使用此程序獲得最佳結果，您應該在 AWS 帳戶. 您的執行個體應包含至少一個 t2.micro 執行個體及其他類型的組合。

若要建立此規則，首先，您將透過在 AWS Lambda 主控台中自訂藍圖來建立 AWS Lambda 函數。然後，您將在中建立自訂 Lambda 規則 AWS Config，並將該規則與函數產生關聯。

主題


- 建立自訂組態規則的 AWS Lambda 函數
- 建立自訂 Lambda 規則以評估 Amazon EC2 執行個體


### 建立自訂組態規則的 AWS Lambda 函數

1. 請登入 AWS Management Console 並開啟 AWS Lambda 主控台，網址為 https://console.aws.amazon.com/lambda/。
2. 在 AWS Management Console 功能表中，確認區域選取器已設定為支援 AWS Config 規則的區域。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在 AWS Lambda 主控台中，選擇 [建立 Lambda 函數]。
4. 選擇 使用藍圖 。在搜尋列中鍵入 config-rule-change-triggered。在篩選結果中選取藍圖，然後選取 設定。
5. 在 Configure triggers (設定觸發條件) 頁面中，選擇 Next (下一步)。
6. 在 基本資訊 頁面上，完成下列步驟：
   a. 針對 Function name (函數名稱)，輸入 **`InstanceTypeCheck`**。
   b. 針對 [執行角色]，選擇 [從 AWS 原則範本建立新角色]。
   c. 針對 Runtime (執行時間)，選擇 Node.js。
   d. 在 角色名稱 中鍵入名稱。
   e. 針對 政策範本，選擇 AWS Config Rules 權限。

f. 對於 Lambda function code function (Lambda 函數程式碼函數)，請保留預先設定的程式碼。您函數的 Node.js 程式碼會在程式碼編輯器中提供。針對此程序，您無須變更程式碼。

g. 確認詳細資訊，接著選擇 建立函數。 AWS Lambda 主控台會顯示您的功能。

7. 若要驗證您的函數已設定正確，請使用下列步驟進行測試：

a. 從 函式概觀 下方的功能表中選擇 測試，然後選擇 設定測試事件。

b. 針對 範本，選擇 AWS Config 組態項目變更通知。

c. 針對 Name (名稱)，輸入名稱。

d. 選擇 [測試]。 AWS Lambda 使用示例事件測試您的函數。若您的函數如預期般正常運作，與下列內容相似的錯誤訊息會出現在 Execution result (執行結果) 下方：

```
{
  "errorType": "InvalidResultTokenException,"
  "errorMessage": "Result Token provided is invalid",
. . .
```

這`InvalidResultTokenException`是預期的，因為您的函數只有在收到來自的結果令牌時才成功運行 AWS Config。結果字符會識別 AWS Config 規則及造成評估的事件，並且結果字符會將評估與規則建立關聯。此異常表示您的函數擁有將結果傳送至 AWS Config的必要許可。否則，會出現下列錯誤訊息：`not authorized to perform: config:PutEvaluations`。若發生此錯誤，請更新您指派給函數的角色，允許 `config:PutEvaluations` 動作，並再次測試您的函數。

建立自訂 Lambda 規則以評估 Amazon EC2 執行個體

1. 開啟主 AWS Config 控台，網址為 https://console.aws.amazon.com/config/。

2. 在 AWS Management Console 功能表中，確認區域選取器設定為您為自訂 Lambda 規則建立 AWS Lambda 函數的相同區域。

3. 在 Rules (規則) 頁面，選擇 Add rule (新增規則)。

4. 在 指定規則類型 頁面上，選擇 建立自訂規則。

5. 在 Configure rule (設定規則) 頁面上，完成下列步驟：

a. 在 Name (名稱) 輸入 **`InstanceTypesAreT2micro`**。

b. 針對 Description (描述)，輸入 **`Evaluates whether EC2 instances are the t2.micro type`**。

c. 在 AWS Lambda function ARN ( 函數 ARN) 中，指定 AWS Lambda 指派給您的函數的 ARN。

> **Note**
>
> 您在此步驟中指定的 ARN 不得包含 `$LATEST` 限定詞。您可以指定沒有版本限定符或除了任何限定符之外`$LATEST`的 ARN。 AWS Lambda 支持功能版本控制，並且每個版本都被分配一個帶有限定符的 ARN。 AWS Lambda 使用最新版本的`$LATEST`限定詞。

d. 針對 觸發類型，選擇 組態有所變更時。

e. 針對 Scope of changes (變更範圍)，選擇 Resources (資源)。

f. 針對 資源，請從 資源類型下拉式清單中選擇 AWS EC2 執行個體。

g. 在「參數」區段中，您必須指定 AWS Lambda 函數評估的規則參數和所需的值。此程序的函數會評估 `desiredInstanceType` 參數。

   在 Key (鍵) 中，輸入 **`desiredInstanceType`**。針對 Value (值)，輸入 **`t2.micro`**。

6. 選擇下一步。在 檢閱和建立 頁面上，驗證規則的詳細資訊，然後選擇 新增函數。您的新規則會顯示在 Rules (規則) 頁面上。

   合規性將顯示評估... 直到從您的 AWS Lambda 函數 AWS Config 收到評估結果。若規則和函數如預期般正常運作，結果摘要便會在幾分鐘之後出現。例如，2 noncompliant resource(s) (2 個不合規資源) 表示您有 2 個執行個體並非 t2.micro 執行個體，Compliant (合規) 結果則表示所有執行個體皆為 t2.micro。您可以使用重新整理按鈕來更新結果。

   如果規則或函數未如預期般正常運作，Compliance (合規) 可能會顯示以下其中一個項目：

   - 未報告結果-根據規則 AWS Config 評估您的資源。規則不適用於範圍內的 AWS 資源，指定的資源已遭刪除，或評估結果已遭刪除。若要取得評估結果，請更新規則、變更其範圍，或選擇 Re-evaluate (重新評估)。

     驗證範圍包含適用於 資源 的 AWS EC2 執行個體，然後再試一次。

   - 沒有資源在範圍內- AWS Config 無法根據此規則評估您記錄的資 AWS 源，因為您的資源都不在規則的範圍內。若要取得評估結果，請編輯規則並變更其範圍，或使用「設定」 頁面新增 AWS Config 要記錄的資源。

     確認 AWS Config 是否正在記錄 EC2 執行個體。

- Evaluations failed (評估失敗) - 如需有助於判斷問題的資訊，請選擇規則名稱以開啟它的詳細資訊頁面，並參閱錯誤訊息。

如果您的規則正常運作並 AWS Config 提供評估結果，您可以瞭解哪些條件會影響規則的符合性狀態。您可以了解哪些資源不合規，以及原因為何 (若有的話)。如需更多詳細資訊，請參閱 檢視相容性資訊與評估結果。

## 自訂 Lambda 規則 (一般範例)

完成下列程序，建立自訂 Lambda 規則。若要建立自訂 Lambda 規則，請先建立包含規則評估邏輯的 AWS Lambda 函數。然後，您會將函數與您在 AWS Config中建立的自訂 Lambda 規則建立關聯。

> **Important**
>
> 作為允許呼叫 Lambda 函數之 AWS Config 權限時的安全性最佳實務，我們強烈建議您使用`sourceARN`和/或在叫用請求中限制 Lambda 資源型政策`sourceAccountId`中的存取權。如需詳細資訊，請參閱 AWS Lambda 資源型政策的安全最佳實務。

內容


- 建立自訂組態規則的 AWS Lambda 函數
- 在中建立自訂規則 AWS Config
- AWS Lambda 資源型政策的安全最佳實務
- 評估其他資源類型


### 建立自訂組態規則的 AWS Lambda 函數

Lambda 函數是您上傳至其中的自訂程式碼 AWS Lambda，由事件來源發佈至該函數的事件所叫用。如果 Lambda 函數與 Config 規則相關聯，則會在規則的觸發程序發生時 AWS Config 叫用該函數。Lambda 函數接著會評估 AWS Config傳送的組態資訊，並傳回評估結果。如需 Lambda 函數的詳細資訊，請參閱《AWS Lambda 開發人員指南》中的函數和事件來源一節。

您可以使用受支援的程式設計語言，為自訂 Lambda 規則建立 Lambda 函數。 AWS Lambda 若要簡化此工作，您可以自訂 AWS Lambda 藍圖或重複使用 AWS Config Rules GitHub 存放庫中的範例函數。

AWS Lambda 藍圖

主 AWS Lambda 控台提供範例函數或藍圖，您可以透過新增自己的評估邏輯來自訂這些函數。當您建立函數時，您可以選擇以下其中一個藍圖：

- config-rule-change-triggered— 當您的 AWS 資源設定變更時觸發。
- config-rule-periodic— 以您選擇的頻率觸發 (例如，每 24 小時)。

AWS Config 規則 GitHub 儲存庫

自訂 Lambda 規則範例函數的公用儲存庫可在 GitHub網頁式程式碼託管和共用服務上取得。示例函數是由社區開發和貢 AWS 獻的。如果您想要使用範例，可以將其程式碼複製到新 AWS Lambda 函式中。若要檢視儲存庫，請參閱 https://github.com/awslabs/aws-config-rules/。

為自訂規則建立函數

1. 請登入 AWS Management Console 並開啟 AWS Lambda 主控台，網址為 https://console.aws.amazon.com/lambda/。
2. 在 AWS Management Console 功能表中，確認區域選取器已設定為支援 AWS Config 規則的區域。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 選擇 Create a Lambda function (建立 Lambda 函數)。
4. 在 [使用藍圖] 頁面上，您可以為 AWS Config 規則選擇其中一個藍圖功能做為起點，或者選擇略過，在沒有藍圖的情況下繼續進行。
5. 在 Configure triggers (設定觸發條件) 頁面中，選擇 Next (下一步)。
6. 在 基本資訊 頁面上，輸入名稱和敘述。
7. 在 Runtime (執行時間) 中，選擇您編寫函數的程式設計語言。
8. 在 Code entry type (程式碼項目類型) 中，選擇您慣用的項目類型。如果您使用藍圖，請保留預先設定的程式碼。
9. 使用您選取的程式碼項目類型所需的方法來提供程式碼。如果您使用的是藍圖，程式碼編輯器中提供的函數程式碼，可讓您自訂並納入您自己的評估邏輯。您的程式碼可以評估呼叫函式時所 AWS Config 提供的事件資料：
   - 對於以config-rule-change-triggered藍圖為基礎的函數，或針對由組態變更觸發的函數，事件資料是變更之 AWS 資源的組態項目或過大的組態項目物件。
   - 對於基於config-rule-periodic藍圖的函數，或者針對以您選擇的頻率觸發的函數，事件資料是 JSON 物件，其中包含有關評估何時觸發的資訊。

- 對於這兩種類型的函數，都會以 JSON 格式 AWS Config 傳遞規則參數。當您在 AWS Config中建立自訂 Lambda 規則時，可以定義要傳遞哪些規則參數。
- 如需呼叫函數時 AWS Config 發佈的事件範例，請參閱AWS Config 規則的範例事件。

10. 針對 執行角色，選擇 從 AWS 政策範本建立新角色。
11. 在 Role name (角色名稱) 中，輸入名稱。
12. 對於 Policy templates (政策範本)，選擇 AWS Config Rules permission ( Config Rules 許可)。
13. 確認詳細資訊，接著選擇 建立函數。

## 在中建立自訂規則 AWS Config

用 AWS Config 於建立自訂 Lambda 規則，並將該規則與 Lambda 函數產生關聯。

### 建立自訂角色

1. 請在以下位置開啟 AWS Config 主控台。 https://console.aws.amazon.com/config/
2. 在 AWS Management Console 功能表中，確認區域選取器設定為您為自訂 Lambda 規則建立 AWS Lambda 函數的相同區域。
3. 在 Rules (規則) 頁面，選擇 Add rule (新增規則)。
4. 在 指定規則類型 頁面上，選擇 建立自訂規則。
5. 在 Configure rule (設定規則) 頁面中，輸入名稱與描述。
6. 在 AWS Lambda function ARN ( 函數 ARN) 中，指定 AWS Lambda 指派給您的函數的 ARN。

> **Note**
>
> 您在此步驟中指定的 ARN 不得包含 `$LATEST` 限定詞。您可以指定沒有版本限定符或除了任何限定符之外`$LATEST`的 ARN。 AWS Lambda 支持功能版本控制，並且每個版本都被分配一個帶有限定符的 ARN。 AWS Lambda 使用最新版本的`$LATEST`限定詞。

7. 在 Trigger type (觸發類型) 中，選擇下列其中一項或兩項：
   - 組態變更 — 在偵測到組態變更時 AWS Config 叫用 Lambda 函數。
   - 定期 — 以您選擇的頻率 AWS Config 叫用 Lambda 函數 (例如，每 24 小時)。
8. 如果規則的觸發器類型包含組態變更，請為 AWS Config 呼叫 Lambda 函數的變更範圍指定下列其中一個選項：
   - 所有變更 — 建立、變更或刪除記錄的任何資源時。 AWS Config

- 資源 – 建立、變更或刪除符合指定類型或加上識別符類型的資源時。
- 標籤 – 建立、變更或刪除含指定標籤的任何資源時。

9. 如果規則的觸發器類型包含「週期性」，請指定 AWS Config 呼叫 Lambda 函數的頻率。
10. 在「參數」區段中，指定 AWS Lambda 函數評估的任何規則參數以及所需的值。
11. 選擇下一步。在 檢閱和建立 頁面上，驗證規則的詳細資訊，然後選擇 Add rule function。您的新規則會顯示在 規則 頁面上。

    合規性將顯示評估... 直到從您的 AWS Lambda 函數 AWS Config 收到評估結果。若規則和函數如預期般正常運作，則結果摘要會在幾分鐘之後出現。您可以使用重新整理按鈕來更新結果。

    如果規則或函數未如預期般正常運作，Compliance (合規) 可能會顯示以下其中一個項目：

    - 未報告結果-根據規則 AWS Config 評估您的資源。規則不適用於範圍內的 AWS 資源，指定的資源已遭刪除，或評估結果已遭刪除。若要取得評估結果，請更新規則、變更其範圍，或選擇 Re-evaluate (重新評估)。

      如果規則未回報評估結果，也會顯示此訊息。
    - 沒有資源在範圍內- AWS Config 無法根據此規則評估您記錄的資 AWS 源，因為您的資源都不在規則的範圍內。您可以選擇 AWS Config 要在 Settings (設定) 頁面上記錄哪些資源。
    - Evaluations failed (評估失敗) - 如需有助於判斷問題的資訊，請選擇規則名稱以開啟它的詳細資訊頁面，並參閱錯誤訊息。

> **Note**
>
> 當您使用 AWS Config 主控台建立自訂 Lambda 規則時，系統會自動為您建立適當的權限。如果您使用建立自訂 Lambda 規則 AWS CLI，則需要 AWS Config 授與使用`aws lambda add-permission`命令叫用 Lambda 函數的權限。如需詳細資訊，請參閱AWS Lambda 開發人員指南中的〈使用以資源為基礎的政策 AWS Lambda (Lambda 函數政策)〉。
> 在 AWS Config 授予叫用 Lambda 函數的權限之前，請參閱下一節AWS Lambda 資源型政策的安全最佳實務。

## AWS Lambda 資源型政策的安全最佳實務

作為安全性最佳實務，為了避免授予整個服務主體名稱 (SPN) 呼叫 Lambda 函數的許可，強烈建議您使用叫用請求中的 `sourceARN` 和/或 `sourceAccountId` 來限制 Lambda 資源型政策中的存取權。

`sourceARN`是正在調用 Lambda 函數的 AWS Config 規則的 ARN。

`sourceAccountId` 是建立規則之使用者的帳戶 ID。

限制 Lambda 資源型政策中的存取權限有助於確保 AWS Lambda 僅代表預期的使用者和案例存取您的資源。

若要新增 SPN 型許可，您需要使用以下 CLI

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com
```

若要新增 SourceAccountId 權限

建立規則之前，您可以使用下列 CLI 將 `sourceAccountId` 型許可新增至資源型政策

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID
```

若要同時新增 SourceArn 和 SourceAccountId 基礎權限

建立規則之後，您可以使用下列 CLI 將 `sourceARN` 型許可新增至資源型政策。這只允許特定規則 ARN 叫用 Lambda 函數。

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID --source-arn ARN of the created config rule
```

評估其他資源類型

您可以建立自訂 Lambda 規則，針對尚未記錄的資源類型執行評估。 AWS Config如果您要評估目前未記錄的其他資源類型的相容性，此功 AWS Config 能非常有用。如需可讓您使用自訂 Lambda 規則來評估的額外資源類型清單，請參閱《AWS 資源類型參考》。

> **Note**
>
> 為未記錄的資源類型建立自訂 Lambda 時 AWS Config，規則必須具有週期性觸發類型。不支援組態變更觸發器類型。如需詳細資訊，請參閱 AWS Config 規則的評估模式與觸發程式型態。

範例

1. 您想要在您的帳戶中評估 Amazon S3 Glacier 保存庫。 AWS Config目前不會記錄 Amazon S3 Glacier 保存庫資源。
2. 您可以建立一個 AWS Lambda 函數來評估 Amazon S3 Glacier 文件庫是否符合您的帳戶需求。
3. 您可以建立名為的自訂 Lambda 規則，evaluate-glacier-vaults然後將 AWS Lambda 函數指派給規則。
4. AWS Config 叫用您的 Lambda 函數，然後根據您的規則評估 Amazon S3 冰川儲存庫。
5. AWS Config 傳回評估，您可以檢視規則的符合性結果。

> **Note**
>
> 您可以在 AWS Config 時間軸中檢視組態詳細資料，並在 AWS Config 主控台中查詢 AWS Config 支援的資源。如果您配置 AWS Config 為記錄所有資源類型，則會自動記錄新支援的資源。如需更多詳細資訊，請參閱 支援的資源類型。

## AWS Config 規則的範例 AWS Lambda 函數和事件

每個自訂 Lambda 規則都與一個 Lambda 相關聯功能，這是包含規則評估邏輯的自訂程式碼。Config 規則的觸發程序發生時 (例如，何時AWS Config偵測組態變更)，AWS Config透過發佈一個叫用規則的 Lambda 函數事件，這是一個 JSON 對象，提供函數評估的配置數據。

如需函數和事件的詳細資訊AWS Lambda，請參閱函數和事件來源在AWS Lambda開發人員指南。

主題

- AWS Config 規則的範例 AWS Lambda 函數 (Node.js)
- AWS Config 規則的範例 AWS Lambda 函數 (Python)
- AWS Config 規則的範例事件

### AWS Config 規則的範例 AWS Lambda 函數 (Node.js)

AWS Lambda 執行函數以回應 AWS 服務所發佈的事件。 AWS Config Custom Lambda 規則的函數會接收由發佈的事件 AWS Config，然後該函數會使用從事件接收並從 AWS Config API 擷取的資料，以評估規則的合規性。針對不同 Config 規則，函數的操作也有所不同。這取決於函數執行的評估是由組態變更或定期觸發而觸發。

如需有關 AWS Lambda 函數中常見模式的資訊，請參閱AWS Lambda 開發人員指南中的程式設計模型。

內容


- 由組態變更觸發之評估的範例函數
- 用於定期評估的範例函數


## 由組態變更觸發之評估的範例函數

AWS Config 當偵測到位於自訂規則範圍內之資源的組態變更時，會叫用類似下列範例的函數。

如果您使用 AWS Config 主控台建立與此範例之函數相關聯的規則，請選擇 [組態變更] 做為觸發器類型。如果您使用 AWS Config API 或 AWS CLI 建立規則，請將`MessageType`屬性設定為`ConfigurationItemChangeNotification`和`OversizedConfigurationItemChangeNotificati`這些設定可讓您在因資源變更而 AWS Config 產生組態項目或過大的組態項目時觸發規則。

此範例會評估您的資源，並檢查執行個體是否符合 `AWS::EC2::Instance` 資源類型。當 AWS Config 產生組態項目或高估容量的組態項目通知時，就會觸發此規則。

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
```

```
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
```

```
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) =>
 {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
 false;
}

// In this example, the resource is compliant if it is an instance and its type matches
 the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
```

```
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is not
 compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
```

```
    });
};
```

函數操作

函數可以在執行時間執行以下操作：

1. 該函數在將event對象 AWS Lambda 傳遞給handler函數時運行。在此範例中，函數會接受選擇性callback參數，該參數會用來將資訊傳回給呼叫者。 AWS Lambda 也會傳遞context物件，其中包含函式在執行時可以使用的資訊和方法。請注意，在較新版本的 Lambda 中已不再使用內容。
2. 此函數會檢查事件的 messageType 為組態項目或高估容量的組態項目，然後傳回組態項目。
3. 處理常式會呼叫 isApplicable 函數，以判斷資源是否已刪除。

   > **Note**
   >
   > 報告已刪除資源的規則，應傳回 NOT_APPLICABLE 的評估結果，以避免不必要的規則評估。

4. 處理常式會呼叫evaluateChangeNotificationCompliance函數，configurationItem並傳遞在事ruleParameters件中 AWS Config 發佈的和物件。

   函數會先評估資源是否為 EC2 執行個體。如果資源不是 EC2 執行個體，則函數會傳回 NOT_APPLICABLE 的合規值。

   接著，函數會評估組態項目中的 instanceType 屬性是否等於 desiredInstanceType 參數值。如果值相同，函數會傳回 COMPLIANT。如果值不相同，函數會傳回 NON_COMPLIANT。
5. 處理常式準備 AWS Config 透過初始化putEvaluationsRequest物件將評估結果傳送至。此物件包含 Evaluations 參數，其可識別符合結果、資源類型和受評估的資源 ID。putEvaluationsRequest物件也包含來自事件的結果 Token，可識別的規則和事件 AWS Config。
6. 處理常式會將物件傳遞至 AWS Config 用config戶端的putEvaluations方法，將評估結果傳送至。

用於定期評估的範例函數

AWS Config 將調用類似下面的例子定期評估的函數。定期評估會按照您在 AWS Config中定義規則時所指定的頻率進行。

如果您使用 AWS Config 主控台建立與此範例之函數相關聯的規則，請選擇「週期性」作為觸發器類型。如果您使用 AWS Config API 或建 AWS CLI 立規則，請將`MessageType`屬性設定為`ScheduledNotification`。

此範例會檢查指定的資源總數是否超過指定上限。

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
 passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount, count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
```

```
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
```

```
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource type.",
 null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count, callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

函數操作

函數可以在執行時間執行以下操作：

1. 該函數在將event對象 AWS Lambda 傳遞給handler函數時運行。在此範例中，函數會接受選擇性callback參數，該參數會用來將資訊傳回給呼叫者。 AWS Lambda 也會傳遞context物件，其中包含函式在執行時可以使用的資訊和方法。請注意，在較新版本的 Lambda 中已不再使用內容。
2. 為了計算指定類型的資源數量，處理常式會呼叫 countResourceTypes 函數，並將從事件接收到的 applicableResourceType 參數傳遞出去。countResourceTypes 函數會呼叫 listDiscoveredResources 方法 (config 用戶端)，這會傳回一份適用的資源識別符清單。函數會使用這份清單的長度來判斷適用資源的數量，並將此計數傳回 給處理常式。
3. 處理常式準備 AWS Config 透過初始化putEvaluationsRequest物件將評估結果傳送至。此物件包含Evaluations參數，可識別符合性結果以及在 AWS 帳戶 事件中發行的參數。您可以使用 Evaluations 參數，將結果套用到 AWS Config支援的任何資源類型。putEvaluationsRequest物件也包含來自事件的結果 Token，可識別的規則和事件 AWS Config。
4. 在 putEvaluationsRequest 物件中，處理常式會呼叫 evaluateCompliance 函數。此函數會測試適用的資源數量是否超過指派給 maxCount 參數的上限，其由事件提供。如果資源數量超過上限，函數會傳回 NON_COMPLIANT。如果資源數量未超過上限，函數會傳回 COMPLIANT。
5. 處理常式會將物件傳遞至 AWS Config 用config戶端的putEvaluations方法，將評估結果傳送至。

## AWS Config 規則的範例 AWS Lambda 函數 (Python)

AWS Lambda 可執行函數，以回應由 AWS 服務發佈的事件。AWS Config 自訂 Lambda 規則的函數會接收由 AWS Config 發佈的事件，然後函數會使用接收自事件及擷取自 AWS Config API 的資料來評估規則合規性。針對不同 Config 規則，函數的操作也有所不同。這取決於函數執行的評估是由組態變更或定期觸發而觸發。

如需 AWS Lambda 函數中常見模式的資訊，請參閱《AWS Lambda 開發人員指南》中的程式設計模型。

內容


- 由組態變更觸發之評估的範例函數
- 用於定期評估的範例函數

由組態變更觸發之評估的範例函數

AWS Config 會在偵測到自訂規則範圍內的資源組態變更時，呼叫類似如下範例的函數。

如果您使用 AWS Config 主控台來建立與此類範例函數相關聯的規則，請選擇 Configuration changes (組態變更) 觸發類型。如果您使用 AWS Config API 或 AWS CLI 來建立規則，請將 `MessageType` 屬性設為 `ConfigurationItemChangeNotification` 和 `OversizedConfigurationItemChangeNotification`。這些設定可讓系統在 AWS Config 因資源變更而產生組態項目或高估容量的組態項目時，觸發您的規則。

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
```

```
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] = json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'], 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')
```

```
# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
```

```
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

### 函數操作

函數可以在執行時間執行以下操作：

1. 該函數會在 AWS Lambda 將 `event` 物件傳遞給 `handler` 函數時執行。在此範例中，函數會接受選擇性 `callback` 參數，該參數會用其將資訊傳回給呼叫者。AWS Lambda 也會傳遞 `context` 物件，其中包含函式在執行時可以使用的資訊和方法。請注意，在較新版本的 Lambda 中已不再使用內容。

2. 此函數會檢查事件的 messageType 為組態項目或高估容量的組態項目，然後傳回組態項目。
3. 處理常式會呼叫 isApplicable 函數，以判斷資源是否已刪除。

> **Note**
>
> 報告已刪除資源的規則，應傳回 NOT_APPLICABLE 的評估結果，以避免不必要的規則評估。

4. 處理常式會呼叫 evaluateChangeNotificationCompliance 函數並傳遞 configurationItem 和 ruleParameters 物件 (由 AWS Config 在事件中發佈)。

   函數會先評估資源是否為 EC2 執行個體。如果資源不是 EC2 執行個體，則函數會傳回 NOT_APPLICABLE 的合規值。

   接著，函數會評估組態項目中的 instanceType 屬性是否等於 desiredInstanceType 參數值。如果值相同，函數會傳回 COMPLIANT。如果值不相同，函數會傳回 NON_COMPLIANT。
5. 處理常式會準備將評估結果傳送到 AWS Config，方法是初始化 putEvaluationsRequest 物件。此物件包含 Evaluations 參數，其可識別符合結果、資源類型和受評估的資源 ID。putEvaluationsRequest 物件也包括來自事件的結果字符，其可識別 AWS Config 的規則和事件。
6. 處理常式會將評估結果傳送給 AWS Config，方法是將物件傳遞至 putEvaluations 方法 (config 用戶端)。

用於定期評估的範例函數

AWS Config 將呼叫類似下列範例的函數，以進行定期評估。定期評估會按照您在 AWS Config 中定義規則時所指定的頻率進行。

如果您使用 AWS Config 主控台來建立與此類範例函數相關聯的規則，請選擇 Periodic (定期) 觸發類型。如果您使用 AWS Config API 或 AWS CLI 來建立規則，請將 MessageType 屬性設為 ScheduledNotification。

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
```

```
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
```

```
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value to
 the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report on
 the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
```

```
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
 resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
 ResultToken=event['resultToken'])
```

函數操作

函數可以在執行時間執行以下操作：

1. 該函數會在 AWS Lambda 將 `event` 物件傳遞給 `handler` 函數時執行。在此範例中，函數會接受選擇性 `callback` 參數，該參數會用其將資訊傳回給呼叫者。AWS Lambda 也會傳遞 `context` 物件，其中包含函式在執行時可以使用的資訊和方法。請注意，在較新版本的 Lambda 中已不再使用內容。
2. 為了計算指定類型的資源數量，處理常式會呼叫 `countResourceTypes` 函數，並將從事件接收到的 `applicableResourceType` 參數傳遞出去。`countResourceTypes` 函數會呼叫 `listDiscoveredResources` 方法 (`config` 用戶端)，這會傳回一份適用的資源識別符清單。函數會使用這份清單的長度來判斷適用資源的數量，並將此計數傳回 給處理常式。
3. 處理常式會準備將評估結果傳送到 AWS Config，方法是初始化 `putEvaluationsRequest` 物件。此物件包含 `Evaluations` 參數，其可識別合規結果和事件中發佈的 AWS 帳

戶。您可以使用 Evaluations 參數，將結果套用到 AWS Config 支援的任何資源類型。putEvaluationsRequest 物件也包括來自事件的結果字符，其可識別 AWS Config 的規則和事件。

4. 在 putEvaluationsRequest 物件中，處理常式會呼叫 evaluateCompliance 函數。此函數會測試適用的資源數量是否超過指派給 maxCount 參數的上限，其由事件提供。如果資源數量超過上限，函數會傳回 NON_COMPLIANT。如果資源數量未超過上限，函數會傳回 COMPLIANT。
5. 處理常式會將評估結果傳送給 AWS Config，方法是將物件傳遞至 putEvaluations 方法 (config 用戶端)。

### AWS Config 規則的範例事件

當規則的觸發程序發生時，會透過發佈事件來 AWS Config 叫用規則的 AWS Lambda 函數。然後通過將事件傳遞給函數的處理程序來 AWS Lambda 執行該函數。

#### 由組態變更觸發之評估的範例事件

AWS Config 當偵測到規則範圍內資源的組態變更時，會發佈事件。下列範例事件顯示規則是由 EC2 執行個體的組態變更觸發。

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

由高估容量組態變更觸發之評估的範例事件

有些資源變更會產生高估容量的組態項目。下列範例事件顯示規則是由 EC2 執行個體的高估容量組態變更觸發。

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

由定期頻率觸發之評估的範例事件

AWS Config 以您指定的頻率 (例如每 24 小時) 評估資源時，會發佈事件。下列範例事件顯示規則是由定期頻率觸發。

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime\":
\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",\"recordVersion
\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
```

```
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

事件屬性

事件的 JSON 物 AWS Config 件包含下列屬性：

`invokingEvent`

觸發規則評估的事件。若事件是因回應資源組態變更而發佈的，則此屬性的值為包含 JSON `configurationItem` 或 `configurationItemSummary` (適用於高估容量的組態項目) 的字串。組態項目代表 AWS Config 偵測到變更時的資源狀態。如需組態項目的範例，請參閱中的`get-resource-config-history` AWS CLI 指令產生的輸出檢視組態歷史記錄。

若事件是因定期評估而發佈，則值為包含 JSON 物件的字串。物件包含觸發評估的相關資訊。

針對每一種事件類型，函數必須使用 JSON 剖析器剖析字串，才能評估其內容，如下列 Node.js 範例所示：

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

函數做為其評估邏輯一部分處理的鍵/值對。您可以在使用 AWS Config 主控台建立自訂 Lambda 規則時定義參數。您也可以使用 `PutConfigRule` AWS Config API 要求或`put-config-rule` AWS CLI 命令中的`InputParameters`屬性來定義參數。

參數的 JSON 程式碼包含在字串中，因此函數必須使用 JSON 剖析器剖析字串，才能評估其內容，如以下 Node.js 範例所示：

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

該函數必須與`PutEvaluations`調用一 AWS Config 起傳遞的令牌。

`eventLeftScope`

Boolean 值，指出要評估的 AWS 資源是否已從規則的範圍中移除。若值為 `true`，則函數會透過在 `PutEvaluations` 呼叫中將 `NOT_APPLICABLE` 做為 `ComplianceType` 屬性的值傳遞，指出可忽略評估。

`executionRoleArn`

指派給的 IAM 角色的 ARN。 AWS Config

`configRuleArn`

AWS Config 指派給規則的 ARN。

`configRuleName`

您指派給導致 AWS Config 發佈事件並呼叫函數之規則的名稱。

`configRuleId`

AWS Config 指派給規則的識別碼。

`accountId`

擁有規則 AWS 帳戶 的識別碼。

`version`

由指派的版本號碼 AWS。如果將屬性 AWS 添加到 AWS Config 事件中，版本將增加。若函數需要只存在於符合或超過特定版本事件中的屬性，則該函數可檢查此屬性的值。

AWS Config 事件的當前版本是 1.0。

# 新增、更新及刪除 AWS Config 規則

您可以使用 AWS Config 主控台或 AWS SDK 來檢視、新增和刪除規則。

## 新增、檢視、更新和刪除規則 (主控台)

規則 頁面會在表格中顯示您的規則和其目前的合規結果。每個規則的結果是評估... 直到 AWS Config 完成根據規則評估資源為止。您可以使用重新整理按鈕來更新結果。 AWS Config 完成評估後，您可以看到符合或不相容的規則和資源類型。如需詳細資訊，請參閱 檢視相容性資訊與評估結果。

> **Note**
>
> AWS Config 僅評估它正在記錄的資源類型。例如，如果您新增啟用 cloudtrail l 的規則，但未記錄 CloudTrail 追蹤資源類型，則 AWS Config 無法評估帳戶中的追蹤是否符合規定或不合規。如需詳細資訊，請參閱 錄製 AWS 資源。

新增規則

新增規則

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 功能表中，確認區域選取器已設定為支援 AWS Config 規則的區域。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在左側導覽中，選擇 規則。
4. 在 Rules (規則) 頁面，選擇 Add rule (新增規則)。
5. 在 指定規則類型 頁面上，透過完成下列步驟來指定規則類型：
   a. 在搜尋欄位中輸入，以透過規則名稱、描述和標籤篩選受管規則清單。例如，輸入 EC2 來傳回評估 EC2 資源類型的規則，或是輸入定期來傳回定期觸發的規則。
   b. 您也可以建立自己的自訂規則。選擇使用 Lambda 建立自訂規則或使用防護建立自訂規則，然後遵循建立 AWS Config 自訂 Lambda 規則或建立 AWS Config 自訂原則規則中的程序。
6. 在 配置規則 頁面中，完成下列步驟以設定規則：
   a. 在 Name (名稱) 欄位中，輸入規則的專屬名稱。
   b. 針對 描述，請輸入規則的描述。
   c. AWS Config 若為「評估」模式，請選擇您要在資源建立與管理程序中評估資源的時間。根據規則， AWS Config 可以在部署資源之前、部署資源之後或兩者之後評估您的資源組態。
      i. 選擇 開啟主動評估，可讓您在部署資源之前，對資源的組態設定執行評估。

         啟用主動式評估之後，您可以使用StartResource評估 API 和 GetResourceEvaluationSummaryAPI 來檢查您在這些命令中指定的資源是否會被您所在地區帳戶中的主動規則標記為 NON_COMPTION。

如需有關使用此命令的詳細資訊，請參閱使用 AWS Config 規則評估資源。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。

ii. 選擇 開啟偵測評估 以評估現有資源的組態設定。

偵測評估有兩種類型的觸發程序：組態有所變更時 和 定期。

A. 如果規則的觸發器類型包含組態變更，請為 AWS Config 呼叫 Lambda 函數的變更範圍指定下列其中一個選項：

- 資源 – 建立、變更或刪除符合指定資源類型或加上識別符類型的資源時。
- 標籤 – 建立、變更或刪除含指定標籤的資源時。
- 所有變更 — 建立、變更或刪除記錄的資源時。 AWS Config

AWS Config 當偵測到符合規則範圍的資源變更時，會執行評估。您可以使用範圍來定義要進行評估的資源。

B. 如果規則的觸發器類型包含「週期性」，請指定 AWS Config 呼叫 Lambda 函數的頻率。

d. 針對 參數，如果您的規則包含參數，則您可以自訂所提供金鑰的值。您的資源必須依循參數這項屬性，才會被視為符合規則。

7. 在 [檢閱並建立] 頁面上，檢閱所有選取項目，然後再將規則新增至您的 AWS 帳戶。如果規則或函數未如預期般正常運作，則 合規 可能會顯示下列其中一個項目：

- 未報告結果-根據規則 AWS Config 評估您的資源。規則不適用於其範圍內的 AWS 資源、刪除指定的資源或評估結果已刪除。若要取得評估結果，請更新規則、變更其範圍，或選擇 Re-evaluate (重新評估)。

  如果規則未回報評估結果，也會顯示此訊息。

- 沒有資源在範圍內- AWS Config 無法根據此規則評估您記錄的資 AWS 源，因為您的資源都不在規則的範圍內。若要取得評估結果，請編輯規則並變更其範圍，或使用「設定」 頁面新增 AWS Config 要記錄的資源。
- Evaluations failed (評估失敗) - 如需有助於判斷問題的資訊，請選擇規則名稱以開啟它的詳細資訊頁面，並參閱錯誤訊息。

## 檢視規則

### 檢視您的規則

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 功能表中，確認區域選取器已設定為支援 AWS Config 規則的區域。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在左側導覽中，選擇 規則。
4. 「規則」(Rules) 頁面會顯示目前在您的規則中的所有規則 AWS 帳戶。其會列出每個規則的名稱、相關聯的修復動作和合規狀態。
   - 選擇 Add rule (新增規則) 以開始建立規則。
   - 請選擇規則以查看其設定，或選擇規則及 檢視詳細資訊。
   - 當規則評估您的資源時，查看規則的合規狀態。
   - 選擇規則，然後選擇 編輯規則 以變更規則的組態設定，並為不合規的規則設定修復動作。

## 更新規則

### 更新規則

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 功能表中，確認區域選取器已設定為支援 AWS Config 規則的區域。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在左側導覽中，選擇 規則。
4. 依序為要更新的規則選擇一項規則及 編輯規則。
5. 修改 編輯規則 頁面上的設定，以視需要變更規則。
6. 選擇 儲存。

## 刪除規則

### 刪除規則

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 功能表中，確認區域選取器已設定為支援 AWS Config 規則的區域。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在左側導覽中，選擇 規則。
4. 從表格選擇您要刪除的規則。
5. 從 動作 下拉式清單中，選擇 刪除規則。
6. 出現提示時，請鍵入 "Delete" (區分大小寫)，然後選擇 刪除。

## 開啟主動評估

您可以使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是 AWS 「非符合」(NON_COMPLIGENTING)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。

資源類型結構描述會說明資源的屬性。您可以在 AWS CloudFormation 註冊表內的「AWS 公共擴展」中或使用以下 CLI 命令找到資源類型模式：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

如需詳細資訊，請參閱《 AWS CloudFormation 使用指南》中的 < 透過 AWS CloudFormation 登錄管理擴充功能 > 以及AWS 資源和屬性類型參考。

> **Note**
>
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

### 開啟主動評估

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。

2. 在 AWS Management Console 功能表中，確認 [地區] 選取器已設定為支援 AWS Config 規則的 [區域]。如需受支援 AWS 區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在左側導覽中，選擇 規則。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。
4. 選擇規則，然後針對您要更新的規則選擇 編輯規則。
5. 針對 評估模式，請選擇 開啟主動評估，這可讓您在部署資源之前，對資源的組態設定執行評估。
6. 選擇 儲存。

啟用主動式評估之後，您可以使用StartResource評估 API 和 GetResourceEvaluationSummaryAPI 來檢查您在這些命令中指定的資源是否會被您所在地區帳戶中的主動規則標記為 NON_COMPTION。

例如，從 StartResourceEvaluation API 開始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您應該會在輸出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然後，使用`ResourceEvaluationId`與 GetResourceEvaluationSummary API 一起檢查評估結果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您應該會收到類似下列的輸出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
```

```
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

若要查看有關評估結果的其他資訊，例如哪些規則將資源標記為「GetComplianceDetailsBy非 _ 相容」，請使用資源 API。

## 檢視、更新或新增及刪除規則 (AWS SDK)

### 檢視規則

下列程式碼範例會示範如何使用`DescribeConfigRules`。

CLI

AWS CLI

若要取得 AWS Config 規則的詳細資訊

下列命令會傳回名為之 AWS Config 規則的詳細資料`InstanceTypesAreT2micro`：

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

輸出：

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
```

```
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考中的DescribeConfig規則。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例會列出帳戶的組態規則，以及選取的屬性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

輸出：

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
```

```
--------------                                    ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                             config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                               config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required        config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程式參考中的DescribeConfig規則。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.
```

```
        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件中的DescribeConfig規則 (Boto3) API 參考。

## 更新或新增規則

下列程式碼範例會示範如何使用`PutConfigRule`。

### CLI

#### AWS CLI

若要新增 AWS 受管理的 Config 規則

以下命令提供 JSON 代碼來添加 AWS 託管 Config 規則：

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`是包含規則組態的 JSON 檔案：

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
```

```
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

對於`ComplianceResourceTypes`屬性，此 JSON 代碼將範圍限制為該`AWS::EC2::Instance`類型的資源，因此 AWS Config 將僅評估 EC2 實例違反規則。由於規則是受管理規則，因此`Owner`屬性會設定為`AWS`，且`SourceIdentifier`屬性會設定為規則識別元`REQUIRED_TAGS`。對於`InputParameters`屬性，會指定規則所需的標籤索引鍵`Owner`、`CostCenter`和。

如果命令成功， AWS Config 不會返回任何輸出。若要驗證規則組態，請執行 describe-config-rules 命令，然後指定規則名稱。

新增客戶管理的 Config 規則

下列命令提供 JSON 程式碼，以新增客戶管理的 Config 規則：

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`是包含規則組態的 JSON 檔案：

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
```

```
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

對於`ComplianceResourceTypes`屬性，此 JSON 代碼將範圍限制為該`AWS::EC2::Instance`類型的資源，因此 AWS Config 將僅評估 EC2 實例違反規則。由於此規則是客戶管理規則，因此`Owner`屬性會設定為`CUSTOM_LAMBDA`，並將`SourceIdentifier`屬性設定為 AWS Lambda 函數的 ARN。該`SourceDetails`對象是必需的。當 AWS Config 呼叫 AWS Lambda 函數以根據規則評估資源時，針對`InputParameters`屬性指定的參數會傳遞至 Lambda 函數。

如果命令成功， AWS Config 不會返回任何輸出。若要驗證規則組態，請執行 describe-config-rules 命令，然後指定規則名稱。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考中的PutConfig規則。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- 如需 API 的詳細資訊，請參閱 AWS SDK 中的PutConfig規則 (Boto3) API 參考。

## 刪除規則

下列程式碼範例會示範如何使用`DeleteConfigRule`。

## CLI

### AWS CLI

#### 刪除 AWS 組 Config 規則

下列命令會刪除名為的 AWS Config 規則`MyConfigRule`：

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考中的DeleteConfig規則。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
```

```
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- 如需 API 的詳細資訊，請參閱 AWS SDK 中的DeleteConfig規則 (Boto3) API 參考。

開啟主動評估 (AWS CLI)

您可以使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是 AWS 「非符合」(NON_COMPLIGENTING)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。

資源類型結構描述會說明資源的屬性。您可以在 AWS CloudFormation 註冊表內的「AWS 公共擴展」中或使用以下 CLI 命令找到資源類型模式：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

如需詳細資訊，請參閱《 AWS CloudFormation 使用指南》中的 < 透過 AWS CloudFormation 登錄管理擴充功能 > 以及AWS 資源和屬性類型參考。

> **Note**
>
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

開啟主動評估

使用 `put-config-rule` 命令並啟用 `EvaluationModes` 的 `PROACTIVE`。

開啟主動評估之後，您可以使用開始資源評估 CLI 命令和取得資源評估- 摘要 CLI 命令，來檢查您在這些命令中指定的資源是否會被您區域中帳戶中的主動規則標記為 NON_COMPLUTION。

例如，從 start-resource-evaluation 命令開始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",
```

```
 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您應該會在輸出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然後，請使用 `ResourceEvaluationId` 與 get-resource-evaluation-summary 來檢查評估結果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您應該會收到類似下列的輸出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

若要查看評估結果的其他資訊，例如哪個規則將資源標記為「NON_COMPLIANT」，請使用 get-compliance-details-by-resource CLI 命令。

> **Note**
>
> 如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。

開啟主動式評估 (API)

您可以使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是 AWS 「非符合」(NON_COMPLIGENTING)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。

資源類型結構描述會說明資源的屬性。您可以在 AWS CloudFormation 註冊表內的「AWS 公共擴展」中或使用以下 CLI 命令找到資源類型模式：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

如需詳細資訊，請參閱《 AWS CloudFormation 使用指南》中的 < 透過 AWS CloudFormation 登錄管理擴充功能 > 以及AWS 資源和屬性類型參考。

> **Note**
>
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

開啟規則的主動評估

使用「PutConfig規則」動作並啟`PROACTIVE`用`EvaluationModes`。

啟用主動式評估之後，您可以使用StartResource評估 API 和 GetResourceEvaluationSummaryAPI 來檢查您在這些命令中指定的資源是否會被您所在地區帳戶中的主動規則標記為 NON_COMPTION。例如，從 StartResourceEvaluation API 開始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您應該會在輸出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然後，使用`ResourceEvaluationId`與 GetResourceEvaluationSummary API 一起檢查評估結果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您應該會收到類似下列的輸出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

若要查看有關評估結果的其他資訊，例如哪些規則將資源標記為「GetComplianceDetailsBy非 _ 相容」，請使用資源 API。

> **Note**
>
> 如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。

## 將規則評估傳送至 Security Hub

新增 AWS Config 規則之後，您也可以將規則評估傳送至 AWS Security Hub。 AWS Config 與 Security Hub 之間的整合可讓您將規則評估與其他錯誤設定和安全性問題一起分類和修復。

### 將規則評估傳送至 Security Hub

若要將規則評估傳送至 Security Hub，您必須先設定 AWS Security Hub 和 AWS Config，然後新增至少一個 AWS Config 受管理或自訂規則。在此之後， AWS Config 立即開始傳送規則評估到 Security Hub。Security Hub 會補充規則評估，並將其轉換為 Security Hub 調查結果。

如需有關此整合的詳細資訊，請參閱 AWS Security Hub 使用者指南中的可用 AWS 服務整合。

# 使用 AWS Config 規則評估您的資源

當您建立自訂規則或使用受管規則時，請根據這些規則 AWS Config 評估您的資源。您可以針對您的規則，執行資源的隨需評估。例如，當您建立自訂規則，並想要檢查 AWS Config 是否正確評估您的資源，或者確定 AWS Lambda 函數的評估邏輯是否有問題時，這會很有幫助。

範例

1. 您可以建立自訂規則，評估您的 IAM 使用者是否擁有作用中的存取金鑰。
2. AWS Config 根據自訂規則評估您的資源。
3. 沒有作用中存取金鑰的 IAM 使用者存在於您的帳戶中。您的規則並未將此資源正確標記為「NON_COMPLIANT」。
4. 您修正規則並再次開始評估。
5. 因為您已修正您的規則，規則會正確評估您的資源，並將 IAM 使用者資源標記為「NON_COMPLIANT」。

將規則新增至帳號時，您可以指定何時在資源建立和管理程序中評估資源。 AWS Config 資源建立和管理程序稱為資源佈建。您可以選擇評估模式，以指定何時在此程序中評估資源。 AWS Config

根據規則， AWS Config 可以在部署資源之前、部署資源之後或兩者之後評估您的資源組態。在部署資源之前對其進行評估，即為主動評估。在部署資源之後對其進行評估，即為偵測評估。

## 主動模式

使用主動評估，在部署資源之前對其進行評估。這可讓您評估一組資源屬性 (如果用來定義資源) 是否為「相容」還是「非符合」(NON_COMPLUTION)，考慮到您在「區域」中的帳戶中擁有的一組主動規則。 AWS

資源類型結構描述會說明資源的屬性。您可以在 AWS CloudFormation 註冊表內的「AWS 公共擴展」中或使用以下 CLI 命令找到資源類型模式：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

如需詳細資訊，請參閱《 AWS CloudFormation 使用指南》中的 < 透過 AWS CloudFormation 登錄管理擴充功能 > 以及AWS 資源和屬性類型參考。

> **Note**
>
> 主動規則不會修復標記為「NON_COMPLIANT」的資源，也不會防止部署這些資源。

評估您的資源

開啟主動評估

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 功能表中，確認 [地區] 選取器已設定為支援 AWS Config 規則的 [區域]。如需受支援 AWS 區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在左側導覽中，選擇 規則。如需支援主動評估的受管規則清單，請參閱按評估模式分類的 AWS Config 受管規則清單。
4. 選擇規則，然後針對您要更新的規則選擇 編輯規則。
5. 針對 評估模式，請選擇 開啟主動評估，這可讓您在部署資源之前，對資源的組態設定執行評估。
6. 選擇 儲存。

> **Note**
>
> 您也可以使用put-config-rule指令來啟用EvaluationModes或使用動作和啟PROACTIVE用的指令來開啟PROACTIVE主PutConfigRule動式評估EvaluationModes。

啟用主動評估之後，您可以使用 StartResourceEvaluationAPI 和 GetResourceEvaluationSummaryAPI 來檢查您在這些命令中指定的資源是否會被您所在地區帳戶中的主動規則標記為「NON_COMPLUTION」。

例如，從 StartResourceEvaluation API 開始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",
```

```
 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您應該會在輸出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然後，使用`ResourceEvaluationId`與 GetResourceEvaluationSummary API 一起檢查評估結果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您應該會收到類似下列的輸出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

若要查看有關評估結果的其他資訊，例如哪些規則將資源標記為「非 _ 相容」，請使用 API。GetComplianceDetailsByResource

## 偵測模式

使用偵測評估來評估已部署的資源。這可讓您評估現有資源的組態設定。

評估您的資源 (主控台)

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 功能表中，檢查區域選擇器是否設定為支援 AWS Config 規則的區域。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。
3. 在導覽窗格中，選擇規則。規則 頁面會顯示每個規則的名稱、相關聯的修復動作和合規狀態。
4. 從清單中選擇規則。
5. 從 動作 下拉式清單中，選擇 重新評估。
6. AWS Config 開始根據您的規則評估資源。

> **Note**
>
> 您可以每分鐘重新評估一次規則。在開始另一個 AWS Config 評估之前，您必須等待完成規則的評估。您無法在規則更新或規則正在刪除的同時執行評估。

評估您的資源 (CLI)

- 使用 start-config-rules-evaluation 命令：

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config 開始根據您的規則評估記錄的資源配置。您也可以在您的請求中指定多個規則：

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

評估您的資源 (API)

使用 StartConfigRulesEvaluation 動作。

# 從AWS Config規則刪除評估結果

在 AWS Config 評估您的規則之後，您可以在 Rules (規則) 頁面或規則的 Rule details (規則詳細資訊) 頁面上看到評估結果。若評估結果不正確，或是您希望再次評估，您可以刪除規則目前的評估結果。例如，若您的規則以不正確的方式評估您的資源，或是您最近從您的帳戶刪除資源，您可以刪除評估結果，並執行新的評估。

## 刪除評估結果 (主控台)

1. 請登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/config/ 的 AWS Config 主控台。
2. 在AWS Management Console功能表中，確認 [地區] 選取器已設定為支援AWS Config規則的 [AWS地區]。如需支援的區域清單，請參閱中的AWS Config區域和端點Amazon Web Services 一般參考。
3. 在導覽窗格中，選擇 Rules (規則)。「規則」頁面會顯示每個規則的名稱、相關聯的修正動作和符合性狀態。
4. 從表格中選擇規則。
5. 從「動作」 下拉式清單中，選擇「刪除結果」。
6. 出現提示時，輸入 [刪除] (此項目區分大小寫)，然後選擇 [刪除]。刪除評估之後，就無法擷取評估。
7. 在評估結果刪除之後，您可以手動啟動新的評估。

## 刪除評估結果 (CLI)

- 使用 delete-evaluation-results 命令。

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

  AWS Config 會刪除規則的評估結果。

## 刪除評估結果

使用 DeleteEvaluationResults 動作。

# 管理組織中所有帳戶的 AWS Config 規則

> **Important**
>
> 您僅能使用 API 或 CLI 建立組織規則。控制台不支持此 AWS Config 操作。

AWS Config 可讓您管理組織 AWS 帳戶 內所有 AWS Config 規則。您可以：

- 集中建立、更新和刪除組織中所有帳戶的 AWS Config 規則。
- 在所有帳戶中部署一組通用 AWS Config 規則，並指定不應在其中建立 AWS Config 規則的帳戶。
- 使用中管理帳戶的 API AWS Organizations 來強制執行管理，方法是確保組織的成員帳戶無法修改基礎 AWS Config 規則。

## 考量事項

針對跨不同區域的部署

跨帳戶部署規則和一致性套件的 API 呼叫是 AWS 區域特定的。如果您想要在其他區域中部署規則，則必須在組織層級將 API 呼叫的內容變更為不同區域。例如，若要在美國東部 (維吉尼亞北部) 部署規則，請將區域變更為美國東部 (維吉尼亞北部)，然後呼叫 `PutOrganizationConfigRule`。

針對組織內的帳戶

如果有新帳戶加入組織，則會將規則或一致性套件部署至該帳戶。當帳戶離開組織時，會移除規則或一致性套件。

如果您在組織管理員帳戶中部署組織規則或一致性套件，然後建立委派的管理員帳戶，並在委派的管理員帳戶中部署組織規則或一致性套件，您將無法從委派管理員帳戶中查看組織管理員帳戶內的組織規則或一致性套件，或從組織管理員帳戶中查看委派管理員帳戶內的組織規則或一致性套件。DescribeOrganizationConfigRules和 DescribeOrganizationConformancePacksAPI 只能查看從呼叫這些 API 的帳戶內部部署的組織相關資源，並與之互動。

新增至組織之新帳戶的重試機制

如果無法使用記錄器，則只有在帳戶新增至組織後，才會持續 7 小時重試部署現有組織規則和一致性套件。如果在將帳戶新增至組織的 7 小時內不存在記錄器，則應建立記錄器。

組織管理帳戶、委派管理員和服務連結角色

如果您使用組織管理帳戶並打算使用委派的系統管理員進行組織部署，請注意， AWS Config 不會自動建立服務連結角色 (SLR)。您必須使用 IAM 個別手動建立服務連結角色 (SLR)。

如果您的管理帳戶沒有 SLR，您將無法從委派的系統管理員帳戶將資源部署到該帳戶。您仍然可以從管理和委派的管理員帳戶將 AWS Config 規則部署到成員帳戶。如需詳細資訊，請參閱 AWS Identity and Access Management (IAM) 使用指南中的使用服務連結角色。

## 部署

若要取得有關如何 AWS Config 與之整合的資訊 AWS Organizations，請參閱《AWS Organizations 使用指南》 AWS Organizations中的AWS Config 和。在您使用下列 API 管理組織 AWS 帳戶 內所有 AWS Config 規則之前，請確定已開啟 AWS Config 錄製檔：

- PutOrganizationConfigRule，新增或更新整個組織的組織組態規則，以評估您的 AWS 資源是否符合您所需的組態。
- DescribeOrganizationConfigRules」，傳回組織組態規則清單。
- GetOrganizationConfigRuleDetailedStatus，針對指定組織組態規則，傳回組織內每個成員帳戶的詳細狀態。
- GetOrganizationCustomRule原則會傳回包含組織設定自訂原則規則之邏輯的原則定義。
- DescribeOrganizationConfigRule狀態，提供組織的組織組態規則部署狀態。
- DeleteOrganizationConfigRule，從該組織中的所有成員帳戶中刪除指定的組織組態規則及其所有評估結果。

## 區域支援

下列區域支援跨組 AWS 織中的成員帳戶部署 AWS Config 規則。

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# 使用規則修復不符合標準的資源 AWS Config

AWS Config 可讓您修復由評估的不符合標準資源。 AWS Config 規則 AWS Config 使用AWS Systems Manager 自動化文件套用補救。這些文件定義要對評估的不符合 AWS 資源執行的動作 AWS Config 規則。您可以使用 AWS Management Console 或使用 API 建立相關的 SSM 文件。

AWS Config 提供一組具有補救動作的受管理自動化文件。您也可以建立自訂自動化文件，並將其與 AWS Config 規則相關聯。

若要對不符合標準的資源套用修復，您可以從預先填入的清單中選擇要關聯的補救動作，或使用 SSM 文件建立您自己的自訂補救動作。 AWS Config 在中提供建議的修復動作清單 AWS Management Console。

在中 AWS Management Console，您可以透過將補救動作與規則相關聯，選擇手動或自動修復不符合資源。 AWS Config 您可以對所有修補動作選擇手動或自動修補。

主題


- 先決條件
- 設定手動修補 (主控台)
- 設定自動修補 (主控台)
- 刪除修補動作 (主控台)
- 管理修補 (API)
- 區域支援


## 先決條件

在您開始於不合規的資源上套用修補之前，必須選取規則並設定規則的修補 (手動或自動)。

## 設定手動修補 (主控台)

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 選擇左側的 規則，然後在 規則 頁面上選擇 新增規則，將新規則新增至規則清單。

   對於現有的規則，請從規則清單中選取不合規的規則，然後選擇 動作 下拉式清單。
3. 從 動作 下拉式清單中，選擇 管理修復。選取「手動修復」，然後從建議清單中選擇適當的修復動作。

   > **Note**
   >
   > 您只能管理非服務連結 AWS Config 規則的補救。如需詳細資訊，請參閱《服務連結 AWS 規則》。

   視選取的修復動作而定，您會看到特定參數，或看不到任何參數。

4. (選用)：如果您想要將不合規資源的資源 ID 傳遞到修復動作，請選擇 資源e ID 參數。若已選取，則該參數會在執行時間替換為要修復的資源 ID。

   每個參數都有靜態值或動態值。如果您未從下拉式清單中選擇特定資源 ID 參數，則可以輸入每個金鑰的值。如果您從下拉式清單中選擇一個資源 ID 參數，則可以輸入所有其他金鑰 (選取的資源 ID 參數除外) 的值。

5. 選擇 儲存。即會顯示 規則 頁面。

`describe-remediation-execution-status`若要疑難排解失敗的修復動作，您可以執行命 AWS 令列介面命令，以取得一組資源修復執行的詳細檢視。詳細資訊包括修復執行步驟的狀態、時間戳記，以及失敗步驟的任何錯誤訊息。

## 設定自動修補 (主控台)

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 選擇左側的 Rules (規則)，然後在 Rules (規則) 頁面上選擇 Add Rule (新增規則)，將規則新增至規則清單。

   對於現有的規則，請從規則清單中選取不合規的規則，然後選擇 動作 下拉式清單。

3. 從 動作 下拉式清單中，選擇 管理修復。選取「自動修復」，然後從建議清單中選擇適當的修復動作。

   > **Note**
   > 您只能管理非服務連結 AWS Config 規則的補救。如需詳細資訊，請參閱《服務連結 AWS 規則》。

   視選取的修復動作而定，您會看到特定參數，或看不到任何參數。

4. 選擇 Auto remediation (自動修補) 來自動修補不合規的資源。

   如果資源在 auto 修復之後仍不合規，您可以將規則設定為再次嘗試 auto 修復。輸入所需的重試次數和秒數。

> **Note**
>
> 多次執行修補指令碼需要支付相關費用。只有在修復失敗時才會發生重試，且會在指定期間內進行；例如，300 秒內重試 5 次。

5. (選用)：如果您想要將不合規資源的資源 ID 傳遞到修復動作，請選擇 資源 ID 參數。若已選取，則該參數會在執行時間替換為要修復的資源 ID。

   每個參數都有靜態值或動態值。如果您未從下拉式清單中選擇特定資源 ID 參數，則可以輸入每個金鑰的值。如果您從下拉式清單中選擇一個資源 ID 參數，則可以輸入所有其他金鑰 (選取的資源 ID 參數除外) 的值。
6. 選擇 儲存。即會顯示 規則 頁面。

疑難排解失敗的補救動作

`describe-remediation-execution-status`若要疑難排解失敗的修復動作，您可以執行命 AWS 令列介面命令，以取得一組資源修復執行的詳細檢視。詳細資訊包括修復執行步驟的狀態、時間戳記，以及失敗步驟的任何錯誤訊息。

即使是符合規定的資源，也可啟動自動補救

如果您使用 Configuration API 或 AWS Config 主控台為特定 AWS Config 規則啟用 auto 修復，它會針對該特定規則啟動所有不符合標準的資源的修正程序。PutRemediationauto 修復程序依賴於定期擷取的合規性資料快照集。在快照排程之間更新的任何不符合標準的資源都將繼續根據上次已知的符合性資料快照進行修復。

這表示在某些情況下，即使是符合規範的資源，也可以啟 auto 修復，因為啟動程序處理器使用的資料庫可能會根據上次已知的相容性資料快照集產生過時的評估結果。

## 刪除修補動作 (主控台)

若要刪除規則，您必須先刪除與該規則關聯的修補動作。

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 選擇左側的 規則，然後在 規則 頁面上，從規則清單中選取規則，然後選擇 檢視詳細資訊。
3. 在 #### 頁面上，移至 修復動作 區段。展開此區段可檢視其他詳細資訊。

4. 在 修復動作 區段中，選擇 刪除 並確認您的刪除動作。

> **Note**
>
> 如果修復正在進行中，將無法刪除修復動作。在選擇刪除修復動作後，將無法擷取修復動作。刪除修復動作不會刪除相關聯的規則。

如果修復動作遭到刪除，則 資源 ID 參數 將為空白並顯示 N/A。在 規則 頁面上，相關聯規則的修復動作欄會顯示 未設定。

# 管理修補 (API)

## 手動修補

使用下列 AWS Config API 動作來管理補救：

- DeleteRemediation配置，刪除修復配置。
- DescribeRemediation組態會傳回一或多個補救組態的詳細資訊。
- DescribeRemediationExecutionStatus，提供一組資源的修正執行詳細檢視，包括狀態、發生修正執行步驟的時間戳記，以及失敗步驟的任何錯誤訊息。
- PutRemediation使用所選目標或動作的特定 AWS Config 規則組態、新增或更新修復組態。
- StartRemediation執行，針對上次已知的修復組態，針對指定的 AWS Config 規則執行隨選修復。

## 自動修補

使用下列 AWS Config API 動作來管理 auto 補救：

- PutRemediation例外狀況會新增例外狀況，或使用特定 AWS Config 規則更新特定資源的現有例外狀況。
- DescribeRemediation例外，會傳回一或多個修正例外的詳細資訊。
- DeleteRemediation例外狀況，會刪除資源金鑰中提到的一或多個補救例外。

# 區域支援

目前，下列區域支援 AWS Config 規則的修正動作：

| 區域名稱 | 區域 | 端點 | 通訊協定 | |
|---|---|---|---|---|
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS | |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS | |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS | |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS | |
| 非洲 (開普敦) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS | |
| 亞太區域 (香港) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS | |
| 亞太區域 (海德拉巴) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS | |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS | |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS | |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS | |
| 亞太區域 (大阪) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS | |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 加拿大西部 (卡加利) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (米蘭) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 歐洲 (西班牙) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 歐洲 (蘇黎世) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| 以色列 (特拉維夫) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| 中東 (巴林) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| 中東 (阿拉伯聯合大公國) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# 故障診斷

如果您無法刪除 AWS Config 規則或收到類似下列內容的錯誤，請檢查下列問題以進行疑難排解：「發生錯誤 AWS Config。」

AWS Identity and Access Management (IAM) 實體具有 DeleteConfigRule API 的許可

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中選擇 [使用者] 或 [角色]。
3. 選擇您用來刪除規則的使用者或角色，然後展開 [權限] 原 AWS Config 則。
4. 在 [權限] 索引標籤中，選擇 [JSON]。
5. 在 JSON 預覽窗格中，確認 IAM 政策允許DeleteConfig規則 API 的許可。

IAM 實體權限界限允許 DeleteConfigRule API

如果 IAM 實體具有許可界限，請確保它允許 DeleteConfigRule API 的許可。

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中選擇 [使用者] 或 [角色]。
3. 選擇您用來刪除 AWS Config 規則的使用者或角色，展開 [權限] 界限，然後選擇 [JSON]。
4. 在 JSON 預覽窗格中，確認 IAM 政策允許DeleteConfig規則 API 的許可。

> **Warning**
>
> IAM 使用者擁有長期登入資料，這會帶來安全風險。為了減輕此風險，我們建議您僅向這些使用者提供執行工作所需的權限，並在不再需要這些使用者時移除這些使用者。

服務控制策略（SCP）允許 API DeleteConfigRule

1. 使用組織的管理帳戶開啟 AWS Organizations 主控台，網址為 https://console.aws.amazon.com/organizations/。
2. 在帳戶名稱中，選擇 AWS 帳戶。
3. 在 [原則] 中，展開 [服務控制原則]，並記下所附加的 SCP 原則。
4. 在頁面頂端，選擇 [原則]。

5. 選取策略，然後選擇 [檢視詳細資料]。
6. 在 JSON 預覽窗格中，確認原則允許DeleteConfig規則 API。

此規則不是服務連結規則

當您啟用安全性標準時， AWS Security Hub 會為您建立服務連結規則。您無法使用刪除這些服務連結規則 AWS Config，而且刪除按鈕會呈現灰色。若要移除服務連結規則，請參閱 Security Hub 使用者指南中的停用安全性標準。

沒有正在進行的修正動作

您無法刪除正在進行修正動作的 AWS Config 規則。依照下列步驟刪除與該規則相關聯的修正動作。然後，請嘗試再次刪除規則。

> **Important**
>
> 僅刪除處於失敗或成功狀態的修正動作。

# 一致性套件

符合性套件是 AWS Config 規則與修正動作的集合，可輕鬆部署為帳戶和區域中的單一實體，或在中的組織中部署。 AWS Organizations

您可以透過編寫包含 AWS Config 受管或自訂規則和修補動作之清單的 YAML 範本，來建立一致性套件。您也可以使用 AWS Systems Manager 文件 (SSM 文件)，將一致性套件範本儲存在 SSM 文件名稱， AWS 並直接部署一致性套件。您可以使用 AWS Config 主控台或 AWS CLI來部署範本。

若要快速開始使用並評估您的 AWS 環境，請使用其中一個範例一致性套件範本。您也可以根據《自訂一致性套件》，從頭開始建立一致性套件 YAML 檔案。

主題


- 必要條件
- 區域支援
- AWS Config 符合性套件中的處理檢查
- 一致性套件範例範本
- 自訂一致性套件
- 在一致性套件儀表板中檢視合規資料
- 檢視一致性套件的合規歷史記錄時間軸
- 使用 AWS Config 主控台部署一致性套件
- 使用 AWS Command Line Interface部署一致性套件
- 管理一致性套件 (API)
- 管理組織中所有帳戶的一致性套件
- 故障診斷


## 必要條件

部署一致性套件之前，請先開啟錄製功能。 AWS Config

### 開始 AWS Config 錄製

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。

2. 在導覽窗格中選擇 Settings (設定)。
3. 若要開始記錄，請在 Recording is off (記錄已關閉) 下方，選擇 Turn on (開啟)。出現提示時，請選擇 繼續。

## 使用一致性套件搭配修補的先決條件

使用具有修正的範例範本部署一致性套件之前，您必須根據修正目標建立適當的資源，例如自動化假設角色和其他 AWS 資源。

如果您有使用 SSM 文件進行修補的現有自動化角色，則可以直接提供該角色的 ARN。如果您有任何資源，則可以在範本中提供這些資源。

> **Note**
>
> 將具有修復的一致性套件部署至組織時，需要指定組織的管理帳戶 ID。否則，在部署組織一致性套件 AWS Config 的期間，系統會自動以成員帳戶 ID 取代管理帳戶 ID。

AWS Config 不支援自動化執行角色的 AWS CloudFormation 內建函式。您必須以字串形式提供角色的確切 ARN。

如需如何傳遞確切 ARN 的詳細資訊，請參閱一致性套件範例範本。使用範例範本時，請更新組織的帳戶 ID 和管理帳戶 ID。

## 將符合性套件與一或多個規則搭配使用的先決條件 AWS Config

在使用一或多個自訂 AWS Config 規則部署符合性套件之前，請先建立適當的資源，例如 AWS Lambda 函數和對應的執行角色。

如果您有現有的自訂 AWS Config 規則，您可以直接提供ARN的 AWS Lambda 函數來建立該自訂規則的另一個執行個體做為套件的一部分。

如果您沒有現有的自訂 AWS Config 規則，您可以建立 AWS Lambda 函數並使用 Lambda 函數的 ARN。如需詳細資訊，請參閱 AWS Config 自訂規則。

如果您的 AWS Lambda 函數存在於不同的 AWS 帳戶，則可以使用適當的跨帳戶 AWS Lambda 函數授權來創建 AWS Config 規則。如需詳細資訊，請參閱如何跨多篇 AWS 帳戶部落格文章集中管理 AWS Config 規則。

### Same account bucket policy

為了能 AWS Config 夠存放一致性套件成品，您需要提供 Amazon S3 儲存貯體並新增以下許可。如需為儲存貯體命名的詳細資訊，請參閱《儲存貯體命名規則》。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

為了能 AWS Config 夠存放一致性套件成品，您需要提供 Amazon S3 儲存貯體並新增以下許可。如需為儲存貯體命名的詳細資訊，請參閱《儲存貯體命名規則》。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> 部署跨帳戶一致性套件時，交付 Amazon S3 儲存貯體的名稱應以 `awsconfigconforms` 開頭。

## 組織一致性套件的先決條件

如果輸入範本具有自動修補組態，請在範本中為該修補指定自動執行角色 ARN。
確定組織的所有帳戶 (管理帳戶和成員帳戶) 中都存在具有指定名稱的角色。在呼叫 `PutOrganizationConformancePack` 之前，您必須在所有帳戶中建立此角色。您可以手動創建此角色，也可以使用 AWS CloudFormation 堆棧集在每個帳戶中創建此角色。

如果您的範本使用 AWS CloudFormation 內建函數匯`Fn::ImportValue`入特定變數，則該變數必須在該組織的所有成員帳戶`Export Value`中定義為一個。

如需自訂規 AWS Config 則，請參閱如何跨多個 AWS 帳戶部落格集中管理 AWS Config 規則以設定適當的權限。

組織儲存貯體政策：

為了能 AWS Config 夠存放一致性套件成品，您需要提供 Amazon S3 儲存貯體並新增以下許可。如需為儲存貯體命名的詳細資訊，請參閱《儲存貯體命名規則》。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> 將一致性套件部署到組織時，所交付 Amazon S3 儲存貯體的名稱應以 `awsconfigconforms` 開頭。

# 區域支援

下列區域支援一致性套件。

| 區域名稱 | 區域 | 端點 | 通訊協定 | |
|---|---|---|---|---|
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS | |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS | |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS | |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS | |
| 亞太區域 (香港) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS | |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS | |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS | |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS | |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS | |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 中東 (巴林) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

下列區域支援跨組 AWS 織中的成員帳戶部署一致性套件。

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# AWS Config 符合性套件中的處理檢查

流程檢查是一種 AWS Config 規則類型，可讓您追蹤需要驗證作為一致性套件一部分的外部和內部任務。您可以將這些檢查新增至現有或新的一致性套件。您可以在單一位置追蹤所有合規性，包括 AWS Config排尿和手動檢查。

透過程序檢查，您可以列出單一位置的要求與動作合規。這些程序檢查有助於增加合規管轄範圍型一致性套件的涵蓋範圍。您可以透過新增全新程序檢查來追蹤需要手動驗證和追蹤的程序和動作，進一步擴充一致性套件。如此可讓符合性套件成為提供有關規範制 AWS Config度之排尿與手動處理之詳細資訊的範本。

您可以在程序檢查時，追蹤並管理不與一致性套件內資源組態變更相關聯的程序合規性。例如，您可以新增程序檢查來追蹤 PCI-DSS 合規性要求，以便將媒體備份儲存在離站位置。您將根據 PCI-DSS 指導方針或貴組織的指引，手動評估其合規性。

區域可用性：提供一致性套件的所有可用區域均可使用程序檢查與 AWS 區域 一 AWS Config 致性套件。如需詳細資訊，請參閱 區域支援。

主題


- 用於建立程序檢查的一致性套件範例範本
- 在一致性套件內包含程序檢查
- 變更程序檢查的合規狀態
- 檢視和編輯程序檢查 (主控台)

## 用於建立程序檢查的一致性套件範例範本

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

請參閱兩個範例範本：獨聯體 AWS 基金會基準 v1.4 級 1 的運營最佳實踐 範本和 獨聯體 AWS 基金會基準第 1.4 版第 2 級的運營最佳實踐 範本。

## 在一致性套件內包含程序檢查

1. 在一致性套件範本中新增程序檢查。請參閱上一個範例範本。

   ```
   Resources:
     ConfigEnabledAllRegions:
       Properties:
         ConfigRuleName: Config-Enabled-All-Regions
         Description: Ensure AWS Config is enabled in all Regions.
         Source:
           Owner: AWS
           SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
       Type: AWS::Config::ConfigRule
   ```

2. 輸入程序檢查的名稱。
3. 輸入程序檢查的敘述。
4. 從 AWS 管理主控台部署一致性套件。如需詳細資訊，請參閱 使用 AWS Config 主控台部署一致性套件。

> **Note**
> 您也可以使用 Command Line Interface (AWS CLI) 來部署一致性套件。如需詳細資訊，請參閱 使用 AWS Command Line Interface部署一致性套件。

# 變更程序檢查的合規狀態

## 變更程序檢查的合規狀態 (主控台)

若要變更程序檢查的符合性狀態 (主控台)

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 瀏覽至「規 AWS Config 則」頁面。
3. 選擇您在範本中指定的程序檢查名稱，以及一致性套件中的識別符。

> **Note**
> 來自相同一致性套件的所有程序檢查，都具有相同的尾碼。

4. 您無法在「規則詳細資訊」頁面上編輯規則，但可以編輯規則的合規性。在「手動合規」區段中，選擇 編輯合規。
5. 從下拉式清單中選擇適當的合規性。
6. (選用) 輸入合規狀態的描述。
7. 選擇儲存。

## 變更程序檢查的合規狀態 (CLI)

若要變更程序檢查 (CLI) 的符合性狀態

您可以使用 AWS Command Line Interface (AWS CLI) 來更新一致性套件內程序檢查的合規性。

若要在本機電腦 AWS CLI 上安裝，請參閱AWS CLI 使用者指南中的安裝 AWS CLI。

如有必要，請鍵入`AWS Config ure`以配置 AWS CLI 以使用提供一 AWS Config 致性包的「 AWS 區域」。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以更新程序檢查您在ComplianceResourceId哪裡的符合性Account ID，並包含規則的名稱。

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. 按 Enter 以執行指令。

### 變更程序檢查 (API) 的合規狀態

若要變更程序檢查 (API) 的符合性狀態

部署完成後，若要更新程序檢查的評估和合規性，請使用 PutExternalEvaluation API。如需詳細資訊，請參閱PutExternal評估。

## 檢視和編輯程序檢查 (主控台)

只有在合規狀態新增至程序檢查之後，您才能檢視程序檢查。選擇特定的一致性套件，即可檢視該一致性套件中的所有程序檢查。您可以在此查看處於相容與不相容狀態的程序檢查清單。

因為這是服務連結規則，所以您無法透過「規則詳細資訊」頁面編輯程序檢查。

> **Note**
> 不過，您可以選擇編輯符合性，然後從「相容」、「不符合」或「不適用」中選取適當的值，來更新流程檢查的符合性。

您可以從新增程序檢查的一致性套件中編輯或刪除程序檢查。

# 一致性套件範例範本

以下是您在主控台中看到的一致性套件 YAML 範本。AWS Config在每個一致性套件範本中，您可以使用一個或多個 AWS Config 規則和修補動作。一致性套件中列出的 AWS Config 規則可以是 AWS Config 受管規則和/或 AWS Config 自訂規則。您可以從中下載所有一致性套件範本。GitHub

> **Important**
>
> 一致性套件提供一般用途的合規框架，可協助您使用受管或自訂 AWS Config 規則與 AWS Config 修補動作，建立安全性、營運或成本優化控管檢查。AWS 一致性套件範例範本旨在協助您利用不同或額外的規則、輸入參數和適合您環境的修補動作，來建立自有的一致性套件。範例範本 (包括與合規標準和產業基準參考指標相關的範本) 並不是為了確保您符合特定控管標準而設計。它們既不能取代您的內部努力，也不能保證您將通過合規性評估。

> **Note**
>
> 建議您檢閱部署一致性套件的區域中可用的規則 (依區域可用性區域列出的AWS Config受管規則清單)，並在部署之前修改該區域中尚未提供的規則範本。

主題

- AWSControl Tower Detective 護衛合規包
- ABS CCIG 2.0 重大工作負載的操作最佳實務
- ABS CCIG 2.0 標準工作負載的操作最佳實務
- ACSC Essential 8 的操作最佳實務
- ACSC ISM 的操作最佳實務
- AI 和 ML 的操作最佳實務
- Amazon API Gateway 的操作最佳實務
- Amazon 的操作最佳實踐 CloudWatch
- Amazon DynamoDB 作最佳實務
- Amazon S3 的操作最佳實踐
- APRA CPG 234 的操作最佳實務
- 資產管理的操作最佳實務
- AWS Backup的操作最佳實務
- AWS身分識別與存取管理的營運最佳作法
- AWS Well-Architected 架構可靠性支柱的營運最佳實務
- Well-Architec AWS ted 的架構安全性支柱的營運最佳實務
- BCP 和 DR 的操作最佳實務

- BNM RMiT 的操作最佳實務
- 加拿大網路安全中心 (CCCS) 中型雲端控制設定檔的最佳營運實務
- 獨聯體 AWS 基金會基準 v1.4 級 1 的運營最佳實踐
- 獨聯體 AWS 基金會基準第 1.4 版第 2 級的運營最佳實踐
- CIS Critical Security Controls v8 IG1 的操作最佳實務
- CIS Critical Security Controls v8 IG2 的操作最佳實務
- CIS Critical Security Controls v8 IG3 的操作最佳實務
- CIS 前 20 項的操作最佳實務
- CISA 網路基礎的操作最佳實務
- 刑事司法資訊服務 (CJIS) 的操作最佳實務
- CMMC 第 1 級的操作最佳實務
- CMMC 第 2 級的操作最佳實務
- CMMC 第 3 級的操作最佳實務
- CMMC 第 4 級的操作最佳實務
- CMMC 第 5 級的操作最佳實務
- CMMC 2.0 第 1 級的操作最佳實務
- CMMC 2.0 第 2 級的操作最佳實務
- 運算服務的操作最佳實務
- 資料復原的操作最佳實務
- 資料庫服務的操作最佳實務
- 資料湖和分析服務的操作最佳實務
- DevOps 的操作最佳實務
- EC2 的操作最佳實務
- 加密和金鑰管理的操作最佳實務
- ENISA 中小企業網路安全指南的操作最佳實務
- Esquema Nacional de Seguridad (ENS) Low 的操作最佳實務
- Esquema Nacional de Seguridad (ENS) Medium 的操作最佳實務
- Esquema Nacional de Seguridad (ENS) High 的操作最佳實務
- FDA 標題 21 CFR 操作最佳實務第 11 部分

- FedRAMP (低) 的操作最佳實務
- FedRAMP (適中) 的操作最佳實務
- FFIEC 的操作最佳實務
- 德國雲端運算合規性標準目錄 (C5) 的最佳作業實務
- Gramm Leach Bliley Act (GLBA) 的操作最佳實務
- GxP EU Annex 11 的操作最佳實務
- HIPAA 安全的操作最佳實務
- IRS 1075 的操作最佳實務
- K-ISMS 的操作最佳實務
- 負載平衡的操作最佳實務
- 日誌的操作最佳實務
- 管理與控管服務的操作最佳實務
- MAS Notice 655 的操作最佳實務
- MAS TRMG 的操作最佳實務
- 監控的操作最佳實務
- NBC TRMG 的操作最佳實務
- NERC CIP BCSI 的操作最佳實務
- NCSC 雲端安全原則的操作最佳實務
- NCSC 網路評估架構的操作最佳實務
- 聯網和內容交付服務的操作最佳實務
- NIST 800-53 修訂版 4 的操作最佳實務
- NIST 800-53 修訂版 5 的最佳操作實務
- NIST 800 171 的操作最佳實務
- NIST 800 172 的操作最佳實務
- NIST 800 181 的操作最佳實務
- NIST 1800 25 的操作最佳實務
- NIST CSF 的操作最佳實務
- NIST 隱私權架構 1.0 版的操作最佳實務
- NYDFS 23 的操作最佳實務

- NZISM 的操作最佳實務
- PCI DSS 3.2.1 的操作最佳實務
- 可公開存取資源的操作最佳實務
- RBI 城市合作銀行 (UCB) 網路安全架構的操作最佳實務
- RBI MD-ITF 的操作最佳實務
- 安全、身分及合規服務的最佳實務
- 無伺服器的操作最佳實務
- 儲存服務的操作最佳實務
- SWIFT CSP 的操作最佳實務
- Amazon Elastic Container Service (Amazon ECS) 的安全最佳實務
- Amazon Elastic File System (Amazon EFS) 的安全最佳實務
- Amazon Elastic Kubernetes Service (Amazon EKS) 的安全最佳實務
- Amazon 的安全最佳實踐 CloudFront
- Amazon OpenSearch 服務的安全最佳實踐
- Amazon Redshift 的安全最佳實務
- Amazon Relational Database Service (Amazon RDS) 的安全最佳實務
- AWS Auto Scaling的安全最佳實務
- AWS CloudTrail的安全最佳實務
- AWS CodeBuild的安全最佳實務
- Amazon ECR 的安全最佳實務
- AWS Lambda的安全最佳實務
- AWS Network Firewall的安全最佳實務
- Amazon 的安全最佳實踐 SageMaker
- AWS Secrets Manager的安全最佳實務
- AWS WAF的安全最佳實務
- 具有修補動作的範例範本

## AWSControl Tower Detective 護衛合規包

該模板可用於 GitHub：Con AWStrol Tower Detective 護欄一致性包。

# ABS CCIG 2.0 重大工作負載的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 ABS 雲端運算實作指南 2.0-材料工作負載和 AWS 受管 Config 規則之間的對映範例。每個 Config 規則都適用於特定 AWS 資源，並與一或多個 ABS 雲端運算實作指南控制項相關。一個《ABS 雲端運算實作指南》控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-2-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| section4a-govern-the-cloud-2-material-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4a-govern-the-cloud-2-standard-workloads | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| section4a-govern-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4a-govern-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4a-govern-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4a-govern-the-cloud-3-material-workloads | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| section4a-govern-the-cloud-3-material-workloads | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-3-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4a-govern-the-cloud-3-standard-workloads | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| section4a-govern-the-cloud-3-standard-workloads | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-3-standard-workloads | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| section4a-govern-the-cloud-3-standard-workloads | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| section4b-design-and-secure-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-3-material-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| section4b-design-and-secure-the-cloud-3-material-workloads | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-material-workloads | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| section4b-design-and-secure-the-cloud-3-material-workloads | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| section4b-design-and-secure-the-cloud-3-material-workloads | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-material-workloads | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即繼續資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| section4b-design-and-secure-the-cloud-4-material-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-4-material-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| section4b-design-and-secure-the-cloud-5-material-workloads | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰於加密期間結束後即輪換。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-material-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-5-material-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| section4b-design-and-secure-the-cloud-5-material-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-material-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| section4b-design-and-secure-the-cloud-6-material-workloads | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰於加密期間結束後即輪換。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-6-material-workloads | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-material-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-8-material-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| section4b-design-and-secure-the-cloud-8-material-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-material-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-8-material-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-9-material-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| section4b-design-and-secure-the-cloud-9-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-material-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-9-material-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| section4b-design-and-secure-the-cloud-9-material-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-material-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-9-material-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-10-material-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4b-design-and-secure-the-cloud-11-material-workloads | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| section4b-design-and-secure-the-cloud-11-material-workloads | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4b-design-and-secure-the-cloud-14-material-workloads | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| section4b-design-and-secure-the-cloud-14-material-workloads | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| section4b-design-and-secure-the-cloud-14-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| section4b-design-and-secure-the-cloud-14-material-workloads | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| section4b-design-and-secure-the-cloud-14-material-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| section4b-design-and-secure-the-cloud-15-material-workloads | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| section4b-design-and-secure-the-cloud-15-material-workloads | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-material-workloads | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| section4b-design-and-secure-the-cloud-15-material-workloads | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4c-run-the-cloud-1-standard-workloads | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| section4c-run-the-cloud-2-material-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-2-material-workloads | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| section4c-run-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| section4c-run-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| section4c-run-the-cloud-2-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原，以及委派許可管理功能。 |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4c-run-the-cloud-2-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4c-run-the-cloud-2-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4c-run-the-cloud-3-standard-workloads | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| section4c-run-the-cloud-3-standard-workloads | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| section4c-run-the-cloud-3-standard-workloads | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| section4c-run-the-cloud-3-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| section4c-run-the-cloud-3-standard-workloads | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4c-run-the-cloud-3-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4c-run-the-cloud-3-standard-workloads | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| section4c-run-the-cloud-3-standard-workloads | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| section4c-run-the-cloud-4-standard-workloads | response-plan-exists-maintained （過程檢查） | 確保已建立、維護事件回應計畫，並將其分發給負責人員。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-4-material-workloads | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| section4c-run-the-cloud-4-material-workloads | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| section4c-run-the-cloud-4-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-4-material-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4c-run-the-cloud-5-standard-workloads | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| section4c-run-the-cloud-5-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| section4c-run-the-cloud-5-standard-workloads | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| section4c-run-the-cloud-5-standard-workloads | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| section4c-run-the-cloud-5-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-6-material-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4c-run-the-cloud-6-material-workloads | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| section4c-run-the-cloud-6-material-workloads | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-6-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| section4c-run-the-cloud-6-material-workloads | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| section4c-run-the-cloud-6-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-6-standard-workloads | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| section4c-run-the-cloud-6-standard-workloads | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| section4c-run-the-cloud-6-standard-workloads | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統的最佳實務。 |

## 範本

範本可在以下網站取得 GitHub：ABS CCIG 2.0 材料工作負載的操作最佳實務。

# ABS CCIG 2.0 標準工作負載的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 ABS 雲端運算實作指南 2.0-標準工作負載和 AWS 受管 Config 規則之間的對應範例。每個 Config 規則都適用於特定 AWS 資源，並與一或多個 ABS 雲端運算實作指南控制項相關。一個《ABS 雲端運算實作指南》控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| section4a-govern-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| section4a-govern-the-cloud-2-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4a-govern-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4a-govern-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4a-govern-the-cloud-3-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4a-govern-the-cloud-3-standard-workloads | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4a-govern-the-cloud-3-standard-workloads | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| section4a-govern-the-cloud-3-standard-workloads | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| section4a-govern-the-cloud-3-standard-workloads | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-1-standard-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| section4b-design-and-secure-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即繼續資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-4-standard-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-5-standard-workloads | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-9-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| section4b-design-and-secure-the-cloud-14-standard-workloads | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| section4c-run-the-cloud-1-standard-workloads | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| section4c-run-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| section4c-run-the-cloud-2-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原，以及委派許可管理功能。 |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4c-run-the-cloud-2-standard-workloads | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| section4c-run-the-cloud-2-standard-workloads | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| section4c-run-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| section4c-run-the-cloud-3-standard-workloads | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| section4c-run-the-cloud-3-standard-workloads | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| section4c-run-the-cloud-3-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| section4c-run-the-cloud-3-standard-workloads | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| section4c-run-the-cloud-3-standard-workloads | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| section4c-run-the-cloud-3-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| section4c-run-the-cloud-3-standard-workloads | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| section4c-run-the-cloud-3-standard-workloads | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| section4c-run-the-cloud-4-standard-workloads | response-plan-exists-maintained （過程檢查） | 確保已建立、維護事件回應計畫，並將其分發給負責人員。 |
| section4c-run-the-cloud-5-standard-workloads | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| section4c-run-the-cloud-5-standard-workloads | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳號 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| section4c-run-the-cloud-5-standard-workloads | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| section4c-run-the-cloud-5-standard-workloads | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| section4c-run-the-cloud-5-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-6-standard-workloads | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| section4c-run-the-cloud-6-standard-workloads | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| section4c-run-the-cloud-6-standard-workloads | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| section4c-run-the-cloud-6-standard-workloads | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統的最佳實務。 |

### 範本

該範本可在以下網站取得 GitHub：ABS CCIG 2.0 標準工作負載的操作最佳實務。

## ACSC Essential 8 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了澳大利亞網絡安全中心（ACSC）基本八成熟度模型和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則都適用於特定 AWS 資源，並與一或多個 ACSC 基本八個控制項相關。一個 ACSC Essential Eight 控制項可以與多項 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。部分 config 規則的映射適用於高階部分 (例如，限制網路安全事件範圍的緩解策略)，而不是更具規定性的部分。

此一致性套件範本範例包含 ACSC Essential 8 控制的映射，ACSC Essential 8 由澳洲聯邦建立，可在 ACSC | Essential Eight 中取得。如需 Creative Commons Attribution 4.0 國際公眾授權下的架構授權和該架構的著作權資訊 (包括保證免責聲明)，請參閱 ACSC | Copyright。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Application_control | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 用性、危及安全性，或在環境中耗用過多資源。 |
| Application_control | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| Application_control | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| Application_control | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| Application_control | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Application_control | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| Application_control | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| Patch_applications | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Patch_applications | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| Patch_applications | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| Patch_applications | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Patch_applications | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| Patch_applications | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| Patch_applications | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Restrict_administrative_privileges | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| Restrict_administrative_privileges | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Restrict_administrative_privileges | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Restrict_administrative_privileges | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |
| Restrict_administrative_privileges | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| Restrict_administrative_privileges | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| Restrict_administrative_privileges | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Restrict_administrative_privileges | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |
| Restrict_administrative_privileges | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Restrict_administrative_privileges | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Restrict_administrative_privileges | rds-instance-iam-authentication-enabled | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體上啟用 AWS 身分和存取管理 (IAM) 身份驗證，以控制對系統和資產的存取。這會強制使用 Secure Sockets Layer (SSL) 來加密往返資料庫的網路流量。您不需要將使用者憑證放在資料庫，因為身分驗證是由外部管理。 |
| Restrict_administrative_privileges | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| Restrict_administrative_privileges | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Restrict_administrative_privileges | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| Restrict_administrative_privileges | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| Restrict_administrative_privileges | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Patch_operating_systems | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| Multi-factor_authentication | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Multi-factor_authentication | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Multi-factor_authentication | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| Multi-factor_authentication | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| Multi-factor_authentication | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Regular_backups | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| Regular_backups | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| Regular_backups | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Regular_backups | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| Regular_backups | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| Regular_backups | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Regular_backups | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| Regular_backups | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| Regular_backups | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Regular_backups | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| Regular_backups | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策來防止刪除復原點，有助於防止意外或故意刪除。 |
| Regular_backups | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Regular_backups | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

### 範本

該模板可用於 GitHub：ACSC 基本 8 的操作最佳實踐。

## ACSC ISM 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供澳洲網路安全中心 (ACSC) 2020-06 年度資訊安全手冊 (ISM) 與 AWS 受管 Config 規則之間的對映範例。每個 Config 規則都會套用至特定的 AWS 資源，並與一或多個 ISM 控制項相關。一個 ISM 控制可以與多個組態規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含 ISM 架構控制的映射，該架構由澳洲聯邦所建立，其可在 Australian Government Information Security Manual 中取得。如需 Creative Commons Attribution 4.0 國際公眾授權下的架構授權和該架構的著作權資訊 (包括保證免責聲明)，請參閱 ACSC | Copyright。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 43 | response-plan-exists-maintained（過程檢查） | 確保已建立、維護事件回應計畫，並將其分發給負責人員。 |
| 252 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 261 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 261 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 261 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 298 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 298 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 298 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 298 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 380 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 459 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 459 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| 459 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 459 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 459 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 459 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 459 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 459 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 459 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 459 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 459 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 459 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 459 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 459 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| 459 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 459 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 459 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 459 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 459 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 459 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 580 | audit-log-policy-exists （過程檢查） | 建立並維護稽核日誌管理政策，以定義組織的日誌記錄要求。這包括但不限於檢閱和保留稽核日誌。 |
| 634 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 859 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 974 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 974 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 1139 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1173 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1173 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1173 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 1173 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1173 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 1228 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 1240 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1240 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 1271 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 1271 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| 1277 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1277 | rds-instance-iam-authentication-enabled | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體上啟用 AWS 身分和存取管理 (IAM) 身份驗證，以控制對系統和資產的存取。這會強制使用 Secure Sockets Layer (SSL) 來加密往返資料庫的網路流量。您不需要將使用者憑證放在資料庫，因為身分驗證是由外部管理。 |
| 1277 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 1380 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1380 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1380 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| 1380 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1380 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 1380 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 1380 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1380 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 1380 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 1380 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1380 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |
| 1380 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| 1380 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 1380 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1380 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |
| 1380 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 1380 | rds-instance-iam-authentication-enabled | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體上啟用 AWS 身分和存取管理 (IAM) 身份驗證，以控制對系統和資產的存取。這會強制使用 Secure Sockets Layer (SSL) 來加密往返資料庫的網路流量。您不需要將使用者憑證放在資料庫，因為身分驗證是由外部管理。 |
| 1380 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1380 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| 1380 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1380 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 1380 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 1388 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1388 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 1401 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 1401 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1401 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 1401 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1401 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1402 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1404 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 1405 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 1405 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 1405 | multi-region-cloudtrail-enabled | MULTI_REGION_CLOUD_TRAIL_ENABLED |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1405 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 1405 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 1405 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 1405 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1405 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 1405 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 1405 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1405 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 1405 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 1405 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1405 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 1405 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 1405 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 1405 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1490 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| 1490 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 1490 | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| 1490 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |
| 1490 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1490 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 1501 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 1504 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1504 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 1504 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 1504 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1504 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1509 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 1509 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1509 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 1509 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 1509 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 1509 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1509 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 1509 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 1509 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1509 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 1509 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 1509 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1509 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 1509 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 1509 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 1509 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1509 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 1511 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 1511 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 1511 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1511 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 1511 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 1511 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1511 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 1511 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 1511 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1511 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 1511 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1511 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| 1511 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 1511 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1511 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 1511 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| 1511 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1515 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 1515 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 1515 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1515 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 1515 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 1515 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1515 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 1515 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 1515 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1515 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| 1515 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 1515 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1515 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 1536 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 1537 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1537 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 1552 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 1552 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1552 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 1552 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1552 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 1579 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1580 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 1580 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1580 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 1650 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 1650 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1650 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 1650 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 1650 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 1650 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1650 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 1650 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 1650 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1650 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 1650 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 1650 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1650 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 1650 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 1650 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 1650 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1650 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 1657 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| 1657 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1657 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1657 | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| 1657 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |
| 1657 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1657 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 1661 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 1661 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1661 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 1661 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 1661 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 1661 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1661 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 1661 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 1661 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1661 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 1661 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 1661 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1661 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 1661 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 1679 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 1679 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1679 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 1679 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1679 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1680 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 1680 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 1680 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1680 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1680 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1681 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 1681 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1681 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 1681 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1681 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1683 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 1683 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 1690 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1690 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1690 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| 1690 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1690 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 1690 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 1690 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1691 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| 1691 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1691 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1691 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 1691 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 1691 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1691 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 1693 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1693 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1693 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| 1693 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1693 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 1693 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 1693 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1694 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 1695 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 1707 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| P1 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P1 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| P3 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| P5 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P7 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| P7 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| P7 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| P7 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P8 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| P9 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P9 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| P9 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| P9 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P9 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| P9 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| P9 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P9 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| P9 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| P9 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P9 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| P9 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| P9 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P9 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| P10 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| P10 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P10 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| P10 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| P10 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| P11 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

### 範本

此範本可在以下網站取得 GitHub：ACSC ISM 的營運最佳作法。

## AI 和 ML 的操作最佳實務

此一致性套件包含以 AI 和 AWS Config ML 為基礎的規則。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可在以下位置獲得 GitHub：AI 和 ML 的操作最佳實踐。

## Amazon API Gateway 的操作最佳實務

此一致性套件包含以內部 Amazon API Gateway 使用情況為基礎的 AWS Config 規則。 AWS如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：Amazon API Gateway 的操作最佳實務。

## Amazon 的操作最佳實踐 CloudWatch

此一致性包包含基於 Amazon CloudWatch 內部使用情況的 AWS Config 規則。 AWS如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可在以下位置獲得 GitHub：Amazon 的操作最佳實踐 CloudWatch。

## Amazon DynamoDB 作最佳實務

該範本可在以下網站取得 GitHub：適用於 Amazon DynamoDB 的操作最佳實務。

## Amazon S3 的操作最佳實踐

該範本可在以下網站取得 GitHub：適用於 Amazon S3 的操作最佳實務。

## APRA CPG 234 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了澳大利亞保誠監管局（APRA）CPG 234 和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 APRA CPG 234 控制項相關。APRA CPG 234 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含 APRA CPG 234 2019 控制的映射，APRA CPG 234 2019 標準由澳洲聯邦建立，可在 Prudential Practice Guide: CPG 234 Information Security 中取得。如需知識共享署名 3.0 授權下的架構授權和該架構的著作權資訊 (包括保證免責聲明)，請參閱 APRA | Copyright。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36a | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 36a | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Syste |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | ms Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 36a | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 36b | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36b | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 36b | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 36b | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36b | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 36b | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| 36b | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36c | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 36c | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 36c | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36c | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 36c | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 36c | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36c | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 36c | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 36c | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| 36d | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36d | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36d | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 36d | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 36d | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 36d | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 36d | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 36d | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 36d | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 36d | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 36d | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 36d | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| 36d | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 36d | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 36d | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 36d | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 36d | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 36d | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 36d | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| 36d | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 36d | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 36d | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 36d | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| 36d | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 36d | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 36d | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 36d | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36d | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 36d | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 36d | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36e | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 36e | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| 36e | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36e | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36e | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36e | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 36e | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36e | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36e | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 36e | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 36e | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36e | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 36e | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 36e | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 36e | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36e | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 36e | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 36e | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 36e | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 36e | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36e | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 36e | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 36e | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |
| 36e | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36e | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 36e | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 36e | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36f | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36f | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36f | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 36f | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 36f | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 36f | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 36f | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 36f | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 36f | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 36f | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 36f | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 36f | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 36f | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 36f | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 36f | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 36f | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 36f | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 36f | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |
| 36f | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36f | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 36f | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 36f | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36g | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 36g | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 36g | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36h | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 36h | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 36h | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36h | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 36h | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 36h | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36h | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 36h | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| 36i | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36i | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 36i | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36i | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 36i | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| 36i | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| 36i | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36i | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 36i | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 36i | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36i | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 36j | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 36j | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36j | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 36j | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 36j | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36j | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 36j | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 36j | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36j | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |
| 36j | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |
| 36j | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36l | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |
| 36l | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流就以處理突然增加的流量。 |
| 36l | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 36l | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36l | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| 36l | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 36l | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36l | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 36l | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 36l | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36l | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 36l | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| 36l | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 36l | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 36l | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 36l | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 39(a)(b)(d) | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 39(a)(b)(d) | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 39(a)(b)(d) | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 40 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 40 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 40 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 40 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 44a | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 44a | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 44a | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 44b | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| 44b | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 44b | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| 44c | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 44c | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 44c | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 44c | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 45 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 45 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 45 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 45 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 45 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 45 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 45 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 45 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 45 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 45 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 45 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 45 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 45 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 45 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 45 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 45 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 45 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 45 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 45 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 45 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 45 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 45 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 45 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 45 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 45 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 45 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 45 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 45 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |
| 45 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 45 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 45 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 47c | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 47c | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 47c | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 47c | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 47c | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 47c | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 47c | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52c | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 52c | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| 52c | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 52c | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 52c | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 52c | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52c | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 52c | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 52c | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52c | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 52c | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 52c | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 52c | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52c | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 52c | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 52c | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 52c | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 52c | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52d | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 52d | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 52d | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 52d | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 52d | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52d | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 52d | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 52d | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52d | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 52d | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 52d | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52d | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 52d | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 52d | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52d | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 52d | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 52d | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 52d | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52d | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |
| 52d | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 52d | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 52d | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52d | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 52e | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 52e | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 53 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 53 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 53 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 53 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 53 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 53 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 53 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 53 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 53 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 53 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 53 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 53 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 53 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 53 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 53 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 53 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 53 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 53 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 53 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 53 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 53 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 53 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 53 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 54 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 54 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 54 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 54 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 54 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| 54 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 54 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 54 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 54 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 54 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 54 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 54 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 54 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 54 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 54 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| 54 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 54 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 54 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 54 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 54 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 54 | rds-snapshot-encrypted | 確保已針對 Amazon Relationa l Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 54 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 54 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 54 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 54 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| 54 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 55 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 55 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 67 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 67 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 67 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 67 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 67 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 67 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 67 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 67 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 67 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 67 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 67 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 67 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 67 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 67 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 67 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 67 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 67 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 67 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 68 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 68 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 73 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 73 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(b)(h) | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AttachmentA_1(b)(h) | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AttachmentA_1(b)(h) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(b)(h) | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AttachmentA_1(b)(h) | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AttachmentA_1(b)(h) | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(b)(h) | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AttachmentA_1(b)(h) | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| AttachmentA_1(b)(h) | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(b)(h) | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AttachmentA_1(c) | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AttachmentA_1(c) | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(e) | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AttachmentA_1(e) | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AttachmentA_1(e) | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(e) | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AttachmentA_1(e) | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AttachmentA_1(e) | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AttachmentA_1(e) | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| AttachmentA_1(e) | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(e) | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AttachmentA_1(e) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AttachmentA_1(e) | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentA_1(e) | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AttachmentA_1(e) | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AttachmentA_1(e) | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AttachmentA_1(e) | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentB_1 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計畫可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |
| AttachmentC_4 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AttachmentC_4 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_4 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| AttachmentC_4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_4 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| AttachmentC_4 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AttachmentC_4 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AttachmentC_4 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_4 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AttachmentC_4 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AttachmentC_4 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_4 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AttachmentC_4 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| AttachmentC_4 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AttachmentC_4 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_4 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AttachmentC_4 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_4 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AttachmentC_4 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AttachmentC_5 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AttachmentC_5 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_5 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AttachmentC_5 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_5 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| AttachmentC_6 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_6 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AttachmentC_6 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| AttachmentC_7(c) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| AttachmentC_7(h) | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_7(h) | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AttachmentC_7(h) | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AttachmentC_7(h) | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| AttachmentC_7(h) | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_7(h) | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AttachmentC_7(h) | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AttachmentC_7(h) | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_7(h) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AttachmentC_7(h) | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AttachmentC_7(h) | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_7(h) | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AttachmentC_7(h) | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| AttachmentC_7(h) | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AttachmentC_7(h) | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_7(i) | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AttachmentC_7(j) | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AttachmentC_7(j) | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_7(j) | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AttachmentC_7(j) | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AttachmentC_8 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| AttachmentC_8 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AttachmentC_8 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_8 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AttachmentC_8 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| AttachmentC_8 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_8 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AttachmentC_8 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AttachmentC_8 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentC_8 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AttachmentC_8 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AttachmentC_8 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AttachmentD_1 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentD_1 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| AttachmentE_4 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| AttachmentE_4 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| AttachmentE_5(d) | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| AttachmentE_1(a)(b)(d) | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| AttachmentE_1(a)(b)(d) | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| AttachmentE_1(a)(b)(d) | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| AttachmentE_1(a)(b)(d) | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| AttachmentE_1(a)(b)(d) | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| AttachmentE_1(a)(b)(d) | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AttachmentE_1(a)(b)(d) | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| AttachmentE_1(a)(b)(d) | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| AttachmentE_1(a)(b)(d) | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AttachmentE_1(a)(b)(d) | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

## 範本

該模板可用於 GitHub：亞太區中央政府 234 的操作最佳實踐。

## 資產管理的操作最佳實務

此一致性套件包含以內部資產管理為基礎的 AWS Config 規則。 AWS如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可在以下位置獲得 GitHub：資產管理的最佳營運實踐。

## AWS Backup的操作最佳實務

此一致性套件包含以內部為基礎的 AWS Config 規則。 AWS Backup AWS如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub： AWS Backup.

## AWS身分識別與存取管理的營運最佳作法

範本位於 GitHub：AWS身分識別與存取管理的作業最佳作法。

## AWS Well-Architected 架構可靠性支柱的營運最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 Amazon Web 服務 Well-Architected 的架構可靠性支柱和 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都適用於特定 AWS 資源，並與支柱的一個或多個設計原則相關。一個 Well-Architected Framework 類別可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-1 | 如何管理服務配額和限制？ 雲端型工作負載架構具有服務配額 (也稱為服務限制)。這些配額的存在是為 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 了防止意外佈建超出所需數量的資源，並限制 API 操作的請求率，以保護服務免於遭到濫用。另外還有一些資源限制，例如可將位元下推到光纖纜線的速率，或實體磁碟的儲存量。 | | 支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| REL-1 | 如何管理服務配額和限制？ 雲端型工作負載架構具有服務配額 (也稱為服務限制)。這些配額的存在是為了防止意外佈建超出所需數量的資源，並限制 API 操作的請求率，以保護服務免於遭到濫用。另外還有一些資源限制，例如可將位元下推到光纖纜線的速率，或實體磁碟的儲存量。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-1 | 如何管理服務配額和限制？ 雲端型工作負載架構具有服務配額 (也稱為服務限制)。這些配額的存在是為了防止意外佈建超出所需數量的資源，並限制 API 操作的請求率，以保護服務免於遭到濫用。另外還有一些資源限制，例如可將位元下推到光纖纜線的速率，或實體磁碟的儲存量。 | ecs-task-definition-memory-hard-limit | 限制 Amazon Elastic Container Service (ECS) 容器的可用記憶體上限，可確保當容器遇到惡意存取時，資源用量不會遭到濫用。 |
| REL-2 | 如何規劃您的網路拓撲？ 工作負載通常存在於多個環境中。其中包括多個雲端環境 (可公開存取與私有)，也可能包含您現有的資料中心基礎設施。這些計畫必須包含網路考量事項，例如系統內部與系統間連線能力、公有 IP 地址管理、私有 IP 地址管理以及網域名稱解析。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-2 | 如何規劃您的網路拓撲？ 工作負載通常存在於多個環境中。其中包括多個雲端環境 (可公開存取與私有)，也可能包含您現有的資料中心基礎設施。這些計畫必須包含網路考量事項，例如系統內部與系統間連線能力、公有 IP 地址管理、私有 IP 地址管理以及網域名稱解析。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-2 | 如何規劃您的網路拓撲？ 工作負載通常存在於多個環境中。其中包括多個雲端環境 (可公開存取與私有)，也可能包含您現有的資料中心基礎設施。這些計畫必須包含網路考量事項，例如系統內部與系統間連線能力、公有 IP 地址管理、私有 IP 地址管理以及網域名稱解析。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-5 | 如何設計分散式系統中的互動以減輕或承受故障？ 分散式系統仰賴通訊網路將伺服器或服務等元件互相連線。儘管這些網路中出現資料遺失或延遲，但工作負載仍必須可靠地運作。分散式系統的元件必須以不會對其他元件或工作負載造成負面影響的方式運作。這些最佳實務可防止故障，並改善平均故障間隔時間 (MTBF)。 | lambda-dlq-check | 啟用此規則可在函數失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | ecs-container-insights-enabled | 監控是維護 Amazon 彈性容器服務 (ECS) 和 AWS 解決方案的可靠性、可用性和效能的重要組成部分。Container Insights 還提供診斷資訊，例如容器重新啟動故障，協助您快速隔離和解決這些故障。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | lambda-dlq-check | 啟用此規則可在函數失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-6 | 如何監控工作負載資源？ 日誌和指標是可深入洞察工作負載運作狀態的強大工具。您可以設定工作負載以監控日誌和指標，並在超過閾值或發生重大事件時傳送通知。監控功能可讓您的工作負載辨識何時超過低效能閾值或發生故障，以便在回應時自動復原。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| REL-7 | 如何設計工作負載以因應需求的變化？ 可擴展的工作負載提供可自動新增或移除資源的彈性，讓資源能夠在任何特定時間點充分滿足目前的需求。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-7 | 如何設計工作負載以因應需求的變化？ 可擴展的工作負載提供可自動新增或移除資源的彈性，讓資源能夠在任何特定時間點充分滿足目前的需求。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| REL-7 | 如何設計工作負載以因應需求的變化？ 可擴展的工作負載提供可自動新增或移除資源的彈性，讓資源能夠在任何特定時間點充分滿足目前的需求。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-8 | 如何實作變更？ 若要部署新功能，並確保工作負載和作業環境正在執行已知軟體，且能夠以可預測的方式修補或取代，必須要有受控變更。如果這些變更不受控制，那麼就很難預測這些變更的影響，也很難解決由於這些變更而產生的問題。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| REL-8 | 如何實作變更？ 若要部署新功能，並確保工作負載和作業環境正在執行已知軟體，且能夠以可預測的方式修補或取代，必須要有受控變更。如果這些變更不受控制，那麼就很難預測這些變更的影響，也很難解決由於這些變更而產生的問題。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-8 | 如何實作變更？ 若要部署新功能，並確保工作負載和作業環境正在執行已知軟體，且能夠以可預測的方式修補或取代，必須要有受控變更。如果這些變更不受控制，那麼就很難預測這些變更的影響，也很難解決由於這些變更而產生的問題。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| REL-8 | 如何實作變更？ 若要部署新功能，並確保工作負載和作業環境正在執行已知軟體，且能夠以可預測的方式修補或取代，必須要有受控變更。如果這些變更不受控制，那麼就很難預測這些變更的影響，也很難解決由於這些變更而產生的問題。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | rds-snapshot-encry pted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-9 | 如何備份資料？ 備份資料、應用程式和組態以滿足您對復原時間點目標 (RTO) 和復原點目標 (RPO) 的要求。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| REL-10 | 如何使用故障隔離來保護工作負載？ 錯誤隔離界限可將工作負載的故障影響限制在有限數量的元件內。界限外部的元件不會受到故障影響。您可以使用多個錯誤隔離界限來限制對工作負載的影響。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-10 | 如何使用故障隔離來保護工作負載？ 錯誤隔離界限可將工作負載的故障影響限制在有限數量的元件內。界限外部的元件不會受到故障影響。您可以使用多個錯誤隔離界限來限制對工作負載的影響。 | clb-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| REL-10 | 如何使用故障隔離來保護工作負載？ 錯誤隔離界限可將工作負載的故障影響限制在有限數量的元件內。界限外部的元件不會受到故障影響。您可以使用多個錯誤隔離界限來限制對工作負載的影響。 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| REL-10 | 如何使用故障隔離來保護工作負載？ 錯誤隔離界限可將工作負載的故障影響限制在有限數量的元件內。界限外部的元件不會受到故障影響。您可以使用多個錯誤隔離界限來限制對工作負載的影響。 | lambda-vpc-multi-az-check | 如果您的 AWS Lambda 函數設定為連線到帳戶中的虛擬私有雲 (VPC)，請在至少兩個不同的可用區域中部署 AWS Lambda 函數，以確保在單一區域中發生服務中斷時，它是您的函數可用來處理事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-10 | 如何使用故障隔離來保護工作負載？ 錯誤隔離界限可將工作負載的故障影響限制在有限數量的元件內。界限外部的元件不會受到故障影響。您可以使用多個錯誤隔離界限來限制對工作負載的影響。 | opensearch-data-node-fault-tolerance | Amazon OpenSearch 服務 (服OpenSearch 務) 至少需要三個資料節點才能達到高可用性和容錯能力。部署具有至少三個資料節點的 OpenSearch Service 網域可確保節點失敗時的叢集作業。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-10 | 如何使用故障隔離來保護工作負載？ 錯誤隔離界限可將工作負載的故障影響限制在有限數量的元件內。界限外部的元件不會受到故障影響。您可以使用多個錯誤隔離界限來限制對工作負載的影響。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| REL-10 | 如何使用故障隔離來保護工作負載？ 錯誤隔離界限可將工作負載的故障影響限制在有限數量的元件內。界限外部的元件不會受到故障影響。您可以使用多個錯誤隔離界限來限制對工作負載的影響。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

### 範本

該模板可用於 GitHub：AWS Well-Architected 的可靠性支柱的操作最佳實踐。

## Well-Architec AWS ted 的架構安全性支柱的營運最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 Amazon Web 服務 Well-Architected 的架構安全支柱和 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都適用於特定 AWS 資源，並與支柱的一個或多個設計原則相關。一個 Well-Architected Framework 類別可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | | 部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SEC-1 | 如何安全地操作工作負載？ 若要安全地操作工作負載，您必須將整體的最佳實務套用到每個安全區域。採用您在組織和工作負載層級於卓越營運中定義的要求和程序，並將其應用於所有區域。掌握最新的產業建議 AWS 和威脅情報，協助您發展威脅模型和控制目標。將安全程序、測試和驗證自動化可讓您擴展安全操作。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | secretsmanager-secret-periodic-rotation | 此規則可確保「 AWS Secrets Manager」密碼已啟用定期輪換。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。預設值為 90 天。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-2 | 如何管理人員和機器的身分？ 處理作業安全 AWS 工作負載時，您需要管理兩種身分識別類型。了解管理和授予存取權所需的身分類型，可協助您確保正確的身分能夠在適當條件下存取正確的資源。人類身分識別：您的管理員、開發人員、操作員和使用者需要身分才能存取您的 AWS 環境和應用程式。這些是您組織的成員，或與您共同作業的外部使用者，以及透過網頁瀏覽器、用戶端應用程式或互動式命令列工具與 AWS 資源互動的使用者。機器識別：您的服務應用程式、作業工具和工作負載需要身分識別才能向 AWS 服務發出要求，例如讀取資料。這些身分識別包括在您 AWS 環境中執行的機器，例如 Amazon EC2 執行個體或 AWS Lambda 函數。您也可以為需要存取權的外部各方管理其機器身 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 分。此外，您可能還有其他電腦需 AWS 要存取您的 AWS 環境。 | | |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 管理員、終端使用者或其他元件都需要存取工作負載的每個元件或資源。請明確定義應該有權存取每個元件的人員和機器，選擇適當的身分類型及驗證和授權方法。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| SEC-3 | 如何管理人員和機器的許可？ 建立通用控制以限制對組織中所有身分的存取。例如，您可以限制對特定 AWS 區域的存取權，或防止操作員刪除常用資源，例如用於中央安全團隊的 IAM 角色 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-3 | 如何管理人員和機器的許可？ 持續監控強調顯示公開和跨帳戶存取的調查結果。僅針對需要此類型存取的資源減少其公開存取和跨帳戶存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | cw-loggroup-retent ion-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-4 | 如何偵測和調查安全事件？ 從日誌和指標中擷取並分析事件，以獲得可見性。請針對安全事件和潛在威脅採取行動，以協助保護工作負載。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SEC-5 | 如何保護網路資源？ 任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | ec2-instance-multiple-eni-check | 此規則會檢查您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體是否擁有多個 ENI。擁有多個 ENI 可能會導致雙主目錄執行個體，也就是具有多個子網路的執行個體。這可能會增加網路安全複雜性，並導致意外的網路路徑和存取。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| SEC-5 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |
| SEC-5 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-5 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SEC-5 | 如何保護網路資源？任何具有某種形式網路連線 (無論是網際網路還是私有網路) 的工作負載，都需要多層防禦來協助防範外部和內部網路型威脅。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ecs-container-insights-enabled | 監控是維持 Amazon 彈性容器服務 (ECS) 和 AWS 解決方案的可靠性、可用性和效能的重要組成部分。Container Insights 還提供診斷資訊，例如容器重新啟動故障，協助您快速隔離和解決這些故障。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-instance-multiple-eni-check | 此規則會檢查您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體是否擁有多個 ENI。擁有多個 ENI 可能會導致雙主目錄執行個體，也就是具有多個子網路的執行個體。這可能會增加網路安全複雜性，並導致意外的網路路徑和存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| SEC-6 | 如何保護運算資源？工作負載中的運算資源需要多層防禦，以協助防範外部和內部威脅。運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。由於有時需要刪除金鑰，因此這個規則可協助檢查所有排定要刪除的金鑰，以防無意中排定金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SEC-8 | 如何保護靜態資料？實作多重控制來保護靜態資料，以降低未經授權存取或處理不當的風險。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SEC-9 | 如何保護傳輸中的資料？ 實作多重控制來保護傳輸中的資料，以降低未經授權存取或遺失的風險。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

### 範本

該模板可在以下位置獲得 GitHub：AWS Well-Architected 的安全支柱的操作最佳實踐。

## BCP 和 DR 的操作最佳實務

此符合性套件包含以內部 BCP 和 DR 為基礎的 AWS Config 規則。 AWS如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網址取得 GitHub：BCP 和 DR 的營運最佳實務。

## BNM RMiT 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供馬來西亞國家銀行 (BNM) 技術風險管理 (RMIT) 與 AWS 託管 Config 規則之間的範例對映。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 BNM RMIT 控制項相關。一個 BNM RMiT 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施， | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.18 | 金融機構必須進行盡職調查，並評估與所用技術相關聯的密碼編譯控制，以便保護資訊的機密性、完整性、驗證、授權和不可否認性。如果金融機構未產生自己的加密金鑰，則金融機構應採取適當的措施，以確保具備管理加密金鑰的可靠控制和流程。如果這涉及依賴第三方評估，則金融機構應考慮此依賴是否與金融機構的風險偏好和承受能力一致。金融機構還必須適當考慮支援密碼編譯控制所需的系統資源，以及降低已加密資料網路流量可見性的風險。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.20 | 金融機構應根據適當的風險層級，將公有密碼編譯金鑰儲存在由憑證授權機構發行的憑證中。與客戶相關聯的憑證須由認可的憑證授權機構發行。金融機構必須確保使用此憑證的驗證和簽章通訊協定實作受到強大保護，以確保所使用對應至使用者憑證的私有密碼編譯金鑰具有法律約束力且不可否認。此憑證的首次發行和後續續約必須與業界最佳實務和適用的法律/法規規範一致。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.20 | 金融機構應根據適當的風險層級，將公有密碼編譯金鑰儲存在由憑證授權機構發行的憑證中。與客戶相關聯的憑證須由認可的憑證授權機構發行。金融機構必須確保使用此憑證的驗證和簽章通訊協定實作受到強大保護，以確保所使用對應至使用者憑證的私有密碼編譯金鑰具有法律約束力且不可否認。此憑證的首次發行和後續續約必須與業界最佳實務和適用的法律/法規規範一致。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.27 | 金融機構必須建立即時監控機制，以追蹤關鍵流程和服務的容量使用率和效能。這些監控機制應該能夠為管理員提供及時可行的警示。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| 10.34 | 金融機構必須確保其關鍵系統的網路服務可靠且沒有 SPOF，以便保護關鍵系統免於潛在網路故障和網路威脅。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.34 | 金融機構必須確保其關鍵系統的網路服務可靠且沒有 SPOF，以便保護關鍵系統免於潛在網路故障和網路威脅。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 10.35 | 金融機構必須建立即時網路頻寬監控流程和對應的網路服務恢復能力指標，以標記由於頻寬擁塞和網路故障所造成的任何頻寬過度使用和系統中斷情況。這包括用於偵測趨勢和異常的流量分析。 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.35 | 金融機構必須建立即時網路頻寬監控流程和對應的網路服務恢復能力指標，以標記由於頻寬擁塞和網路故障所造成的任何頻寬過度使用和系統中斷情況。這包括用於偵測趨勢和異常的流量分析。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 10.35 | 金融機構必須建立即時網路頻寬監控流程和對應的網路服務恢復能力指標，以標記由於頻寬擁塞和網路故障所造成的任何頻寬過度使用和系統中斷情況。這包括用於偵測趨勢和異常的流量分析。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.35 | 金融機構必須建立即時網路頻寬監控流程和對應的網路服務恢復能力指標，以標記由於頻寬擁塞和網路故障所造成的任何頻寬過度使用和系統中斷情況。這包括用於偵測趨勢和異常的流量分析。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 10.36 | 金融機構必須確保設計和實作支援關鍵系統的網路服務，以確保資料的機密性、完整性和可用性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.36 | 金融機構必須確保設計和實作支援關鍵系統的網路服務，以確保資料的機密性、完整性和可用性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.36 | 金融機構必須確保設計和實作支援關鍵系統的網路服務，以確保資料的機密性、完整性和可用性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 10.36 | 金融機構必須確保設計和實作支援關鍵系統的網路服務，以確保資料的機密性、完整性和可用性。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 10.36 | 金融機構必須確保設計和實作支援關鍵系統的網路服務，以確保資料的機密性、完整性和可用性。 | nlb-cross-zone-load-balancing-enabled | 為 Network Load Balancer (NLB) 啟用跨區域負載平衡，以協助維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.38 | 金融機構必須確保保留足夠且相關的網路裝置日誌至少三年，以供調查和鑑識之用。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取許可和授權，方法是確保 IAM 使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有 IAM 使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為 IAM 使用者要求 MFA 來減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.51 | 金融機構在使用雲端服務時，必須為客戶和交易對手資訊和專屬資料實作適當的保護措施，以防止未經授權的洩漏和存取。這應該包括保留託管在雲端上之所有客戶專屬資料以及交易對手資訊、專屬資料和服務的擁有權、控制權和管理權，包括相關的密碼編譯金鑰管理。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedAc tionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取許可和授權，方法是確保 IAM 使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有 IAM 使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為 IAM 使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.52 | 金融機構必須實作適當的存取控制政策，以便識別、驗證和授權使用者 (內部使用者以及第三方服務供應商等外部使用者)。這必須同時解決與未經授權存取其技術系統之風險層級相符的邏輯和實體技術存取控制問題 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 10.53(b)(h)(i) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務；(h) 限制及控制多位使用者共用使用者 ID 和密碼；及 (i) 控制通用使用者 ID 命名慣例的使用，改為更能識別個人的 ID。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.53(b) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務； | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 10.53(b) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務； | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.53(b) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務； | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 10.53(b) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務； | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.53(b) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務； | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 10.53(b) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務； | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取許可和授權，方法是確保 IAM 使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.53(b) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(b) 採用「最低權限」存取權限，或基於「必須擁有」，只將最低足夠許可授予合法使用者，以便其執行職務； | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.53(c)(f) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(c) 採用有時限的存取權限，限制在特定時段內進行存取 (包括授予服務供應商的存取權限)；(f) 對關鍵活動 (包括遠端存取) 採用更強大的驗證 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.53(f)(h) | 在遵守第 10.52 項時，金融機構應考慮將以下原則納入其存取控制政策：(f) 對關鍵活動 (包括遠端存取) 採用更強大的驗證；(h) 限制及控制多位使用者共用使用者 ID 和密碼 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有 IAM 使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為 IAM 使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 10.53(f)(h) | 在遵守第 10.54 項時，金融機構應考慮將以下原則納入其存取控制政策：(f) 對關鍵活動 (包括遠端存取) 採用更強大的驗證；(h) 限制及控制多位使用者共用使用者 ID 和密碼 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.53(f)(h) | 在遵守第 10.54 項時，金融機構應考慮將以下原則納入其存取控制政策：(f) 對關鍵活動 (包括遠端存取) 採用更強大的驗證；(h) 限制及控制多位使用者共用使用者 ID 和密碼 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 10.54 | 金融機構必須採用強大的驗證程序，以確保使用中身分的真確性。認證機制應與功能的重要性相稱，並至少採用這三個基本認證因素中的一項或多項，即使用者知道的資訊 (例如密碼、PIN)、使用者所擁有的東西 (例如智慧卡、安全裝置)，以及使用者所擁有的東西 (例如生物特徵，例如指紋或視網膜圖案)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有 IAM 使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為 IAM 使用者要求 MFA 來減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.54 | 金融機構必須採用強大的驗證程序，以確保使用中身分的真確性。認證機制應與功能的重要性相稱，並至少採用這三個基本認證因素中的一項或多項，即使用者知道的資訊 (例如密碼、PIN)、使用者所擁有的東西 (例如智慧卡、安全裝置)，以及使用者所擁有的東西 (例如生物特徵，例如指紋或視網膜圖案)。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 10.54 | 金融機構必須採用強大的驗證程序，以確保使用中身分的真確性。認證機制應與功能的重要性相稱，並至少採用這三個基本認證因素中的一項或多項，即使用者知道的資訊 (例如密碼、PIN)、使用者所擁有的東西 (例如智慧卡、安全裝置)，以及使用者所擁有的東西 (例如生物特徵，例如指紋或視網膜圖案)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.55 | 金融機構應定期審查和調整其密碼實務，以更有彈性地應對不斷進化的攻擊。這包括有效且安全地產生密碼。必須有適當的控制措施來檢查所建立密碼的強度。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.56 | 依賴多個要素的驗證方法通常比單一要素系統更難入侵。有鑑於此，建議金融機構正確設計和實作 (特別是在高風險或「單一登入」系統中) 多重要素驗證 (MFA)，此驗證方法不僅更可靠，也提供更強大的詐騙阻嚇 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有 IAM 使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為 IAM 使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 10.56 | 依賴多個要素的驗證方法通常比單一要素系統更難入侵。有鑑於此，建議金融機構正確設計和實作 (特別是在高風險或「單一登入」系統中) 多重要素驗證 (MFA)，此驗證方法不僅更可靠，也提供更強大的詐騙阻嚇 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.56 | 依賴多個要素的驗證方法通常比單一要素系統更難入侵。有鑑於此，建議金融機構正確設計和實作 (特別是在高風險或「單一登入」系統中) 多重要素驗證 (MFA)，此驗證方法不僅更可靠，也提供更強大的詐騙阻嚇 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取許可和授權，方法是確保 IAM 使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 10.59 | 金融機構必須確保 (a) 有效管理和監控整個企業系統的存取控制；以及 (b) 記錄關鍵系統中的使用者活動，以供稽核與調查。活動日誌必須及時維護至少三年並定期審查。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.60 | 為了滿足第 10.59 項的要求，大型金融機構必須 (a) 部署身分存取管理系統，以有效管理和監控使用者對整個企業系統的存取；以及 (b) 部署自動化稽核工具來標記任何異常。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 10.60 | 為了滿足第 10.61 項的要求，大型金融機構必須 (a) 部署身分存取管理系統，以有效管理和監控使用者對整個企業系統的存取；以及 (b) 部署自動化稽核工具來標記任何異常。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.60 | 為了滿足第 10.61 項的要求，大型金融機構必須 (a) 部署身分存取管理系統，以有效管理和監控使用者對整個企業系統的存取；以及 (b) 部署自動化稽核工具來標記任何異常。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.61 | 金融機構必須確保關鍵系統不會在具有已知安全漏洞或 end-of-life （EOL）技術系統的過時系統上運行。針對這點，金融機構必須明確指派責任給確定的職能：(a) 以便及時持續監控和實作最新的修補程式版本；以及 (b) 識別生命週期即將結束的關鍵技術系統，以便採取進一步補救措施。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 10.61 | 金融機構必須確保關鍵系統不會在具有已知安全漏洞或 end-of-life （EOL）技術系統的過時系統上運行。針對這點，金融機構必須明確指派責任給確定的職能：(a) 以便及時持續監控和實作最新的修補程式版本；以及 (b) 識別生命週期即將結束的關鍵技術系統，以便採取進一步補救措施。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.61 | 金融機構必須確保關鍵系統不會在具有已知安全漏洞或 end-of-life （EOL）技術系統的過時系統上運行。針對這點，金融機構必須明確指派責任給確定的職能：(a) 以便及時持續監控和實作最新的修補程式版本；以及 (b) 識別生命週期即將結束的關鍵技術系統，以便採取進一步補救措施。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 10.61 | 金融機構必須確保關鍵系統不會在具有已知安全漏洞或 end-of-life （EOL）技術系統的過時系統上運行。針對這點，金融機構必須明確指派責任給確定的職能：(a) 以便及時持續監控和實作最新的修補程式版本；以及 (b) 識別生命週期即將結束的關鍵技術系統，以便採取進一步補救措施。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.61 | 金融機構必須確保關鍵系統不會在具有已知安全漏洞或 end-of-life （EOL）技術系統的過時系統上運行。針對這點，金融機構必須明確指派責任給確定的職能：(a) 以便及時持續監控和實作最新的修補程式版本；以及 (b) 識別生命週期即將結束的關鍵技術系統，以便採取進一步補救措施。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.64(a) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(a) 客戶及交易對手資訊與交易的機密性和完整性 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.64(b) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(b) 透過管道和裝置提供服務的可靠性，並將服務中斷降至最低 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(b) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(b) 透過管道和裝置提供服務的可靠性，並將服務中斷降至最低 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 10.64(b) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(b) 透過管道和裝置提供服務的可靠性，並將服務中斷降至最低 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 10.64(b) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(b) 透過管道和裝置提供服務的可靠性，並將服務中斷降至最低 | nlb-cross-zone-load-balancing-enabled | 為平衡 NetworkLoad 器 (NLB) 啟用跨區域負載平衡，以協助維持適當的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(b) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(b) 透過管道和裝置提供服務的可靠性，並將服務中斷降至最低 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(b) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(b) 透過管道和裝置提供服務的可靠性，並將服務中斷降至最低 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(b) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(b) 透過管道和裝置提供服務的可靠性，並將服務中斷降至最低 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(d) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(d) 足夠的稽核記錄並監控異常交易 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.64(e) | 金融機構在提供數位服務時，必須實作強大的技術安全控制，以確保下列事項：(e) 能夠在事件或服務中斷之前識別並回復至復原點 | s3-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Simple Storage Service (S3) 儲存貯體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.7 | 金融機構必須部署有效的工具，以支援持續且主動的監控，並及時偵測其技術基礎設施中的異常活動。監控範圍必須涵蓋所有關鍵系統，包括支援的基礎設施。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.7 | 金融機構必須部署有效的工具，以支援持續且主動的監控，並及時偵測其技術基礎設施中的異常活動。監控範圍必須涵蓋所有關鍵系統，包括支援的基礎設施。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 11.8 | 金融機構必須確保其網路安全操作持續預防和偵測其安全控制的任何潛在入侵或其安全狀態的弱化。對於大型金融機構，這必須包括每季對支援所有關鍵系統的外部和內部網路元件執行漏洞評估。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.8 | 金融機構必須確保其網路安全操作持續預防和偵測其安全控制的任何潛在入侵或其安全狀態的弱化。對於大型金融機構，這必須包括每季對支援所有關鍵系統的外部和內部網路元件執行漏洞評估。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 11.18(c)(f) | SOC 必須能夠執行下列功能：(c) 漏洞管理；(f) 提供情境感知以偵測敵人和威脅，包括威脅情報分析和操作，以及監控入侵指標 (IOC)。這包括進階行為分析，可偵測無簽章和無檔案的惡意軟體，並識別可能造成安全威脅的異常 (包括在端點和網路層)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.18(c)(f) | SOC 必須能夠執行下列功能：(c) 漏洞管理；(f) 提供情境感知以偵測敵人和威脅，包括威脅情報分析和操作，以及監控入侵指標 (IOC)。這包括進階行為分析，可偵測無簽章和無檔案的惡意軟體，並識別可能造成安全威脅的異常 (包括在端點和網路層)。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.18(c)(f) | SOC 必須能夠執行下列功能：(c) 漏洞管理；(f) 提供情境感知以偵測敵人和威脅，包括威脅情報分析和操作，以及監控入侵指標 (IOC)。這包括進階行為分析，可偵測無簽章和無檔案的惡意軟體，並識別可能造成安全威脅的異常 (包括在端點和網路層)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 附錄 5.1 | 定期審查所有安全裝置的組態和規則設定。使用自動化工具來審查和監控組態和規則設定的變更。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 5.1 | 定期審查所有安全裝置的組態和規則設定。使用自動化工具來審查和監控組態和規則設定的變更。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 附錄 5.5(b) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（b）使用安全通道，例如傳輸層安全（TLS）和虛擬私人網絡（VPN）IPsec | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 5.5(b) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（b）使用安全通道，例如傳輸層安全（TLS）和虛擬私人網絡（VPN）IPsec | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 附錄 5.5(b) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（b）使用安全通道，例如傳輸層安全（TLS）和虛擬私人網絡（VPN）IPsec | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 附錄 5.5(b) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（b）使用安全通道，例如傳輸層安全（TLS）和虛擬私人網絡（VPN）IPsec | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 5.5(b) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（b）使用安全通道，例如傳輸層安全（TLS）和虛擬私人網絡（VPN）IPsec | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 附錄 5.5(b) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（b）使用安全通道，例如傳輸層安全（TLS）和虛擬私人網絡（VPN）IPsec | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 附錄 5.5(c) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（c）部署具有足夠周邊防禦和保護的測試服務器，例如防火牆，IPS 和防病毒。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 5.5(c) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（c）部署具有足夠周邊防禦和保護的測試服務器，例如防火牆，IPS 和防病毒。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 附錄 5.5(c) | 確保 server-to-server 外部網絡連接的保安控制包括以下內容：（c）部署具有足夠周邊防禦和保護的測試服務器，例如防火牆，IPS 和防病毒。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 5.6 | 確保伺服器遠端存取的安全控制包括：(a) 僅限存取已強化且鎖定的端點裝置；(b) 使用安全通道，例如 TLS 和 VPN IPSec；(c) 部署具有適當周邊防禦和保護的「閘道」伺服器，例如防火牆、IPS 和防毒軟體；以及 (d) 在遠端存取到期時立即關閉相關的連接埠。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 附錄 5.6 | 確保伺服器遠端存取的安全控制包括：(a) 僅限存取已強化且鎖定的端點裝置；(b) 使用安全通道，例如 TLS 和 VPN IPSec；(c) 部署具有適當周邊防禦和保護的「閘道」伺服器，例如防火牆、IPS 和防毒軟體；以及 (d) 在遠端存取到期時立即關閉相關的連接埠。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 5.6 | 確保伺服器遠端存取的安全控制包括：(a) 僅限存取已強化且鎖定的端點裝置；(b) 使用安全通道，例如 TLS 和 VPN IPSec；(c) 部署具有適當周邊防禦和保護的「閘道」伺服器，例如防火牆、IPS 和防毒軟體；以及 (d) 在遠端存取到期時立即關閉相關的連接埠。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 附錄 5.6 | 確保伺服器遠端存取的安全控制包括：(a) 僅限存取已強化且鎖定的端點裝置；(b) 使用安全通道，例如 TLS 和 VPN IPSec；(c) 部署具有適當周邊防禦和保護的「閘道」伺服器，例如防火牆、IPS 和防毒軟體；以及 (d) 在遠端存取到期時立即關閉相關的連接埠。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 5.6 | 確保伺服器遠端存取的安全控制包括：(a) 僅限存取已強化且鎖定的端點裝置；(b) 使用安全通道，例如 TLS 和 VPN IPSec；(c) 部署具有適當周邊防禦和保護的「閘道」伺服器，例如防火牆、IPS 和防毒軟體；以及 (d) 在遠端存取到期時立即關閉相關的連接埠。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 附錄 5.6 | 確保伺服器遠端存取的安全控制包括：(a) 僅限存取已強化且鎖定的端點裝置；(b) 使用安全通道，例如 TLS 和 VPN IPSec；(c) 部署具有適當周邊防禦和保護的「閘道」伺服器，例如防火牆、IPS 和防毒軟體；以及 (d) 在遠端存取到期時立即關閉相關的連接埠。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 1 (a) 部分 | 金融機構應設計強大的雲端架構，並確保該設計符合預期應用程式的相關國際標準。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 附錄 10 第 B - 1 (b) 部分 | 我們鼓勵金融機構採用零信任原則，透過採用「假設違規」思維模式、 defense-in-depth 透過微分段、「預設拒絕」、「最低特權」存取權限，以及在適用情況下進行深度檢查和持續驗證，以提供網路彈性架構。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 附錄 10 第 B - 1 (b) 部分 | 我們鼓勵金融機構採用零信任原則，透過採用「假設違規」思維模式、 defense-in-depth 透過微分段、「預設拒絕」、「最低特權」存取權限，以及在適用情況下進行深度檢查和持續驗證，以提供網路彈性架構。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 1 (b) 部分 | 我們鼓勵金融機構採用零信任原則，透過採用「假設違規」思維模式、 defense-in-depth 透過微分段、「預設拒絕」、「最低特權」存取權限，以及在適用情況下進行深度檢查和持續驗證，以提供網路彈性架構。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 附錄 10 第 B - 1 (b) 部分 | 我們鼓勵金融機構採用零信任原則，透過採用「假設違規」思維模式、 defense-in-depth 透過微分段、「預設拒絕」、「最低特權」存取權限，以及在適用情況下進行深度檢查和持續驗證，以提供網路彈性架構。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 1 (c) 部分 | 金融機構應使用最新的網路架構方法以及適當的網路設計概念和解決方案來管理和監控精細的網路安全，並使用集中式網路佈建來管理雲端網路環境的複雜性。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 附錄 10 第 B - 1 (c) 部分 | 金融機構應使用最新的網路架構方法以及適當的網路設計概念和解決方案來管理和監控精細的網路安全，並使用集中式網路佈建來管理雲端網路環境的複雜性。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 附錄 10 第 B - 1 (d) 部分 | 金融機構應建立並利用安全且加密的通訊管道，將實體伺服器、應用程式或資料移轉至雲端平台。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 1 (d) 部分 | 金融機構應建立並利用安全且加密的通訊管道，將實體伺服器、應用程式或資料移轉至雲端平台。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 附錄 10 第 B - 1 (f) i) 部分 | 金融機構越來越常使用應用程式介面 (API) 來與外部應用程式服務供應商互連，而得以提高新服務交付的效率。不過，這可能會增加網路受攻擊面，任何管理不善的情況都可能會擴大資訊安全事件的影響。金融機構應確保其 API 具有嚴格的管理和控制機制，其中包括：i) API 應設計成具備服務恢復能力以避免單點故障的風險，並使用適當的存取控制安全地進行設定； | api-gwv2-authorization-type-configured | 確保您的 Amazon API Gateway v2 API 路由已設定授權類型，以防止未經授權存取基礎後端資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 1 (f) ii) 部分 | 金融機構越來越常使用應用程式介面 (API) 來與外部應用程式服務供應商互連，而得以提高新服務交付的效率。不過，這可能會增加網路受攻擊面，任何管理不善的情況都可能會擴大資訊安全事件的影響。金融機構應確保其 API 具有嚴格的管理和控制機制，其中包括：ii) 應透過適當的事件回應措施來追蹤和監控 API 以防止網路攻擊，並於不再使用時及時汰除。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 1 (f) ii) 部分 | 金融機構越來越常使用應用程式介面 (API) 來與外部應用程式服務供應商互連，而得以提高新服務交付的效率。不過，這可能會增加網路受攻擊面，任何管理不善的情況都可能會擴大資訊安全事件的影響。金融機構應確保其 API 具有嚴格的管理和控制機制，其中包括：ii) 應透過適當的事件回應措施來追蹤和監控 API 以防止網路攻擊，並於不再使用時及時汰除。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 附錄 10 第 B - 2 (b) ii) 部分 | 金融機構應持續利用增強的雲端功能來改善雲端服務的安全；此外，建議金融機構：ii) 使用不可變的基礎設施實務來部署服務，透過使用軟體的最新穩定版本建立新環境，藉以降低失敗的風險。雲端環境的持續監控應包括自動偵測不可變基礎設施的變更，以改善合規性審查並應對不斷進化的網路攻擊 | cloudformation-stack-notification-check | 若要偵測基礎 AWS 資源的意外變更，請確保您的 CloudFormation 堆疊設定為將事件通知傳送至 Amazon SNS 主題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 3 (b) vi) 部分 | 金融機構應確保適當設定、強化及監控虛擬機器和容器映像。這包括：vi) 對儲存的映像進行安全監控，以防止未經授權的存取和變更。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 附錄 10 第 B - 5 (a) i) 部分 | 為了能夠有效復原，金融機構應確保擴展現有的備份和復原程序以涵蓋雲端服務，其中包括：i) 在雲端採用的規劃階段定義和正規化備份和復原策略； | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 附錄 10 第 B - 5 (a) i) 部分 | 為了能夠有效復原，金融機構應確保擴展現有的備份和復原程序以涵蓋雲端服務，其中包括：i) 在雲端採用的規劃階段定義和正規化備份和復原策略； | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (a) i) 部分 | 為了能夠有效復原，金融機構應確保擴展現有的備份和復原程序以涵蓋雲端服務，其中包括：i) 在雲端採用的規劃階段定義和正規化備份和復原策略； | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 附錄 10 第 B - 5 (a) i) 部分 | 為了能夠有效復原，金融機構應確保擴展現有的備份和復原程序以涵蓋雲端服務，其中包括：i) 在雲端採用的規劃階段定義和正規化備份和復原策略； | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (a) i) 部分 | 為了能夠有效復原，金融機構應確保擴展現有的備份和復原程序以涵蓋雲端服務，其中包括：i) 在雲端採用的規劃階段定義和正規化備份和復原策略； | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 附錄 10 第 B - 5 (a) i) 部分 | 為了有效執行復原功能，金融機構應確保擴展現有的備份和復原程序以涵蓋雲端服務，其中包括：i) 在雲端採用的規劃階段定義和正規化備份和復原策略； | s3-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Simple Storage Service (S3) 儲存貯體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (b) 部分 | 金融機構應確保定期測試備份和還原程序，以驗證復原功能。備份程序的頻率應與系統的重要性和系統的復原點目標 (RPO) 相符。如果備份失敗，金融機構應立即採取補救措施。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (c) i) 部分 | 金融機構應確保虛擬機器和容器有足夠的備份和復原，包括備份組態設定（適用於 IaaS 和 PaaS，如有關），其中包括以下內容：i) 確保能夠按照業務復原目標指定的恢復虛擬機器和容器； point-in-time | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (d) i) 部分 | 金融機構應評估雲端服務的恢復能力要求，並確定與系統重要性相符的適當措施，以確保極端不利情況下的服務可用性。金融機構應考慮以風險為基礎的方法，並逐步採取適當的緩解控制措施，以確保服務可用性並降低集中風險。可行的選擇包括：i) 利用雲端服務的高可用性和備援功能，確保生產資料中心在不同的可用區域擁有備援容量； | autoscaling-multiple-az | 為了確保高可用性，請確保將 Auto Scaling 群組設定為跨多個可用區域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (d) i) 部分 | 金融機構應評估雲端服務的恢復能力要求，並確定與系統重要性相符的適當措施，以確保極端不利情況下的服務可用性。金融機構應考慮以風險為基礎的方法，並逐步採取適當的緩解控制措施，以確保服務可用性並降低集中風險。可行的選擇包括：i) 利用雲端服務的高可用性和備援功能，確保生產資料中心在不同的可用區域擁有備援容量； | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (d) i) 部分 | 金融機構應評估雲端服務的恢復能力要求，並確定與系統重要性相符的適當措施，以確保極端不利情況下的服務可用性。金融機構應考慮以風險為基礎的方法，並逐步採取適當的緩解控制措施，以確保服務可用性並降低集中風險。可行的選擇包括：i) 利用雲端服務的高可用性和備援功能，確保生產資料中心在不同的可用區域擁有備援容量； | lambda-vpc-multi-az-check | 如果您的 AWS Lambda 函數設定為連線到帳戶中的虛擬私有雲 (VPC)，請在至少兩個不同的可用區域中部署 AWS Lambda 函數，以確保在單一區域中發生服務中斷時，它是您的函數可用來處理事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (d) i) 部分 | 金融機構應評估雲端服務的恢復能力要求，並確定與系統重要性相符的適當措施，以確保極端不利情況下的服務可用性。金融機構應考慮以風險為基礎的方法，並逐步採取適當的緩解控制措施，以確保服務可用性並降低集中風險。可行的選擇包括：i) 利用雲端服務的高可用性和備援功能，確保生產資料中心在不同的可用區域擁有備援容量； | nlb-cross-zone-load-balancing-enabled | 為平衡 NetworkLoad 器 (NLB) 啟用跨區域負載平衡，以協助維持適當的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (d) i) 部分 | 金融機構應評估雲端服務的恢復能力要求，並確定與系統重要性相符的適當措施，以確保極端不利情況下的服務可用性。金融機構應考慮以風險為基礎的方法，並逐步採取適當的緩解控制措施，以確保服務可用性並降低集中風險。可行的選擇包括：i) 利用雲端服務的高可用性和備援功能，確保生產資料中心在不同的可用區域擁有備援容量； | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 5 (d) i) 部分 | 金融機構應評估雲端服務的恢復能力要求，並確定與系統重要性相符的適當措施，以確保極端不利情況下的服務可用性。金融機構應考慮以風險為基礎的方法，並逐步採取適當的緩解控制措施，以確保服務可用性並降低集中風險。可行的選擇包括：i) 利用雲端服務的高可用性和備援功能，確保生產資料中心在不同的可用區域擁有備援容量； | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | eks-secrets-encrypted | 為了協助保護靜態資料，請確保您的 Amazon Elastic Kubernetes Service (EKS) 叢集已設定為對 Kubernetes 密碼進行加密。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 附錄 10 第 B - 8 (a) 部分 | 金融機構應實作適當且相關的加密技術，以保護儲存在雲端之敏感資料的機密性和完整性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 8 (d) 部分 | 隨著雲端採用的使用率增加，管理許多用於保護資料的加密金鑰變得越來越複雜，並且可能會為金融機構帶來新的挑戰。金融機構應採用全方位且集中的金鑰管理方法，包括使用集中式金鑰管理系統，以安全且可擴展的方式處理金鑰的產生、儲存和分發。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 附錄 10 第 B - 8 (d) 部分 | 隨著雲端採用的使用率增加，管理許多用於保護資料的加密金鑰變得越來越複雜，並且可能會為金融機構帶來新的挑戰。金融機構應採用全方位且集中的金鑰管理方法，包括使用集中式金鑰管理系統，以安全且可擴展的方式處理金鑰的產生、儲存和分發。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 9 (a) ii) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來訪問管理平面，其中可能包括以下內容：ii）實施「最小權限」和強大的多因素身份驗證（MFA），例如強密碼，軟令牌，特權訪問管理工具和製作者檢查器功能； | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 9 (a) ii) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來訪問管理平面，其中可能包括以下內容：ii）實施「最小權限」和強大的多因素身份驗證（MFA），例如強密碼，軟令牌，特權訪問管理工具和製作者檢查器功能； | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有 IAM 使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。透過為 IAM 使用者要求 MFA 來減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 9 (a) ii) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來訪問管理平面，其中可能包括以下內容：ii）實施「最小權限」和強大的多因素身份驗證（MFA），例如強密碼，軟令牌，特權訪問管理工具和製作者檢查器功能； | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 9 (a) ii) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來訪問管理平面，其中可能包括以下內容：ii）實施「最小權限」和強大的多因素身份驗證（MFA），例如強密碼，軟令牌，特權訪問管理工具和製作者檢查器功能； | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 附錄 10 第 B - 9 (a) iii) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來限制對管理平面的存取，其中可能包括：iii) 為特殊權限使用者採用精細的權利分配； | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 9 (a) iii) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來限制對管理平面的存取，其中可能包括：iii) 為特殊權限使用者採用精細的權利分配； | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 附錄 10 第 B - 9 (a) iv) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來限制對管理平面的存取，其中可能包括：iv) 持續監控特殊權限使用者所執行的活動； | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 9 (a) iv) 部分 | 管理平面是傳統基礎設施與雲端運算之間的主要安全差異，預設支援遠端存取。此存取層可能很容易受到網路攻擊，從而破壞整個雲端部署的完整性。有鑑於此，金融機構應確保使用強大的控制來限制對管理平面的存取，其中可能包括：iv) 持續監控特殊權限使用者所執行的活動； | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 附錄 10 第 B - 12 (a) 部分 | 金融機構應根據本政策文件「資料外洩防護」一節 (第 11.14 至 11.16 項) 的要求，保護在雲端服務中託管的資料，包括擴大端點使用量 (如果金融機構允許員工使用自己的裝置存取敏感資料)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 12 (a) 部分 | 金融機構應根據本政策文件「資料外洩防護」一節 (第 11.14 至 11.16 項) 的要求，保護在雲端服務中託管的資料，包括擴大端點使用量 (如果金融機構允許員工使用自己的裝置存取敏感資料)。 | macie-status-check | Amazon Macie 是一項資料安全服務，使用機器學習 (ML) 和模式比對來探索和協助保護儲存在 Amazon Simple Storage Service (S3) 儲存貯體中的敏感資料。 |
| 附錄 10 第 B - 14 (c) i) 部分 | 金融機構在制定 CIRP 時，應考慮以下其他措施：i) 增強其偵測安全檢測安全缺口事件的能力，以實現有效的事件管理，包括在暗網上偵測資料外洩的能力； | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 附錄 10 第 B - 14 (c) i) 部分 | 金融機構在制定 CIRP 時，應考慮以下其他措施：i) 增強其偵測安全檢測安全缺口事件的能力，以實現有效的事件管理，包括在暗網上偵測資料外洩的能力； | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

### 範本

該範本可在以下網站取得 GitHub：BNM RMIT 的營運最佳實務。

## 加拿大網路安全中心 (CCCS) 中型雲端控制設定檔的最佳營運實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供加拿大網路安全中心 (CCCS) 中型雲端控制設定檔與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CCCS 中型雲端控制設定檔控制項相關。一個 CCCS 中型雲端控制設定檔控制項可與多個 Config 規則相關聯。如需與這些映射相關的詳細資訊和指導，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) 帳戶管理 \| 自動化系統帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(3) | AC-2(3) 帳戶管理 \| 停用非作用中帳戶 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(3) | AC-2(3) 帳戶管理 \| 停用非作用中帳戶 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-2(4) | AC-2(4) 帳戶管理 \| 自動稽核動作 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-AC-2(4) | AC-2(4) 帳戶管理 \| 自動稽核動作 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) 帳戶管理 \| 自動稽核動作 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AC-2(4) | AC-2(4) 帳戶管理 \| 自動稽核動作 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) 帳戶管理 \| 自動稽核動作 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| CCCS-fPBMM-AC-2(4) | AC-2(4) 帳戶管理 \| 自動稽核動作 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) 帳戶管理 \| 自動稽核動作 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Managemen t (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-AC-3.A | AC-3.A 存取強制執行 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-4(21) | AC-4(21) 資訊流強制執行 \| 實體/邏輯分離資訊流 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A 資訊流強制執行 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-AC-5.A | AC-5.A 職責分離 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A 職責分離 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A 職責分離 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A 職責分離 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A 職責分離 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-6(1) | AC-6(1) 最低權限 \| 授權存取安全功能 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(1) | AC-6(1) 最低權限 \| 授權存取安全功能 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-6(1) | AC-6(1) 最低權限 \| 授權存取安全功能 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(1) | AC-6(1) 最低權限 \| 授權存取安全功能 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-AC-6(1) | AC-6(1) 最低權限 \| 授權存取安全功能 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) 最低權限 \| 非安全功能的非權限存取 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-6(2) | AC-6(2) 最低權限 \| 非安全功能的非權限存取 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) 最低權限 \| 非安全功能的非權限存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-AC-6(2) | AC-6(2) 最低權限 \| 非安全功能的非權限存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) 最低權限 \| 非安全功能的非權限存取 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-AC-6(5) | AC-6(5) 最低權限 \| 權限帳戶 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(5) | AC-6(5) 最低權限 \| 權限帳戶 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-AC-6(5) | AC-6(5) 最低權限 \| 權限帳戶 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(5) | AC-6(5) 最低權限 \| 權限帳戶 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-AC-6(9) | AC-6(9) 最低權限 \| 稽核權限功能的使用情形 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-AC-6(9) | AC-6(9) 最低權限 \| 稽核權限功能的使用情形 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) 最低權限 \| 稽核權限功能的使用情形 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AC-6(9) | AC-6(9) 最低權限 \| 稽核權限功能的使用情形 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) 最低權限 \| 稽核權限功能的使用情形 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| CCCS-fPBMM-AC-6(9) | AC-6(9) 最低權限 \| 稽核權限功能的使用情形 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) 最低權限 \| 稽核權限功能的使用情形 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AC-6(10) | AC-6(10) 最低權限 \| 禁止非權限使用者執行權限功能 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(10) | AC-6(10) 最低權限 \| 禁止非權限使用者執行權限功能 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-6(10) | AC-6(10) 最低權限 \| 禁止非權限使用者執行權限功能 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(10) | AC-6(10) 最低權限 \| 禁止非權限使用者執行權限功能 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-AC-6(10) | AC-6(10) 最低權限 \| 禁止非權限使用者執行權限功能 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A 最低權限 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) 遠端存取 \| 自動化監控/控制 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AC-17(2) | AC-17(2) 遠端存取 \| 使用加密保護機密性/完整性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-17(2) | AC-17(2) 遠端存取 \| 使用加密保護機密性/完整性 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(2) | AC-17(2) 遠端存取 \| 使用加密保護機密性/完整性 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CCCS-fPBMM-AC-17(2) | AC-17(2) 遠端存取 \| 使用加密保護機密性/完整性 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(2) | AC-17(2) 遠端存取 \| 使用加密保護機密性/完整性 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-17(2) | AC-17(2) 遠端存取 \| 使用加密保護機密性/完整性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-AC-17(3) | AC-17(3) 遠端存取 \| 受管存取控制點 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(4) | AC-17(4) 遠端存取 \| 權限命令/存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-AC-17(4) | AC-17(4) 遠端存取 \| 權限命令/存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(4) | AC-17(4) 遠端存取 \| 權限命令/存取 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A 遠端存取 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA 遠端存取 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B 遠端存取 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A 稽核事件 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B 稽核事件 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C 稽核事件 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D 稽核事件 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) 稽核記錄內容 \| 其他稽核資訊 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A 稽核記錄內容 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AU-5.A | AU-5.A 對稽核處理失敗的回應 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-5.B | AU-5.B 對稽核處理失敗的回應 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) 審核檢閱、分析和報告 \| 流程整合 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-AU-6(1) | AU-6(1) 審核檢閱、分析和報告 \| 流程整合 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) 審核檢閱、分析和報告 \| 流程整合 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-6(1) | AU-6(1) 審核檢閱、分析和報告 \| 流程整合 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) 審核檢閱、分析和報告 \| 流程整合 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) 稽核檢閱、分析和報告 \| 整合流程 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) 稽核檢閱、分析和報告 \| 建立稽核儲存庫關聯 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AU-7(1) | AU-7(1) 減少稽核與產生報告 \| 自動處理 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B 時間戳記 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-9(2) | AU-9(2) 保護稽核資訊 \| 不同實體系統/元件的稽核備份 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| CCCS-fPBMM-AU-9(2) | AU-9(2) 保護稽核資訊 \| 不同實體系統/元件的稽核備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-9(2) | AU-9(2) 保護稽核資訊 \| 不同實體系統/元件的稽核備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| CCCS-fPBMM-AU-9.A | AU-9.A 保護稽核資訊 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-9.A | AU-9.A 保護稽核資訊 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-AU-9.A | AU-9.A 保護稽核資訊 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-11.A | AU-11.A 保留稽核記錄 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| CCCS-fPBMM-AU-11.B | AU-11.B 保留稽核記錄 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| CCCS-fPBMM-AU-11.C | AU-11.C 保留稽核記錄 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助稽核安全性和存取，也可協助診斷可用性問題。 |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A 產生稽核 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C 產生稽核 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) 系統互連 \| 外部網路連線限制 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | api-gw-xray-enabled | AWS X-Ray 會收集應用程式所提供請求的相關資料，並提供工具供您檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。確保 X-Ray 已啟用，因此您不僅可以查看有關請求和響應的詳細信息，還可以查看應用程序對下游 AWS 資源，微服務，數據庫和 HTTP Web API 進行的調用的詳細信息。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A 內部系統連線 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-CM-2.A | CM-2.A 基準組態 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A 基準組態 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| CCCS-fPBMM-CM-2.A | CM-2.A 基準組態 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以利設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A 基準組態 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| CCCS-fPBMM-CM-2.A | CM-2.A 基準組態 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A 基準組態 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A 基準組態 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-3.A | CM-3.A 組態變更控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.A | CM-3.A 組態變更控制 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-3.B | CM-3.B 組態變更控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.B | CM-3.B 組態變更控制 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-3.C | CM-3.C 組態變更控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.C | CM-3.C 組態變更控制 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-3.D | CM-3.D 組態變更控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.D | CM-3.D 組態變更控制 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-3.E | CM-3.E 組態變更控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.E | CM-3.E 組態變更控制 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-3F | CM-3F 組態變更控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3F | CM-3F 組態變更控制 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-3.G | CM-3.G 組態變更控制 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.G | CM-3.G 組態變更控制 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼的作用中時間，並可能降低其洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| CCCS-fPBMM-CM-5(1) | CM-5(1) 變更存取限制 \| 強制執行自動存取/稽核 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) 變更存取限制 \| 限制生產/營運權限 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A 變更存取限制 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6(1) | CM-6(1) 組態設定 \| 自動化中央管理/應用程式/驗證 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6(1) | CM-6(1) 組態設定 \| 自動化中央管理/應用程式/驗證 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| CCCS-fPBMM-CM-6(1) | CM-6(1) 組態設定 \| 自動化中央管理/應用程式/驗證 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CCCS-fPBMM-CM-6.A | CM-6.A 組態設定 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CCCS-fPBMM-CM-6.B | CM-6.B 組態設定 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CCCS-fPBMM-CM-6.C | CM-6.C 組態設定 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CCCS-fPBMM-CM-6.D | CM-6.D 組態設定 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-7.A | CM-7.A 最少功能 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-CM-7.A | CM-7.A 最少功能 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-7.B | CM-7.B 最少功能 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-CM-7.B | CM-7.B 最少功能 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(1) | CM-8(1) 資訊系統元件庫存清單 \| 於安裝/移除期間更新 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8(1) | CM-8(1) 資訊系統元件庫存清單 \| 於安裝/移除期間更新 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(2) | CM-8(2) 資訊系統元件庫存清單 \| 自動化維護 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8(2) | CM-8(2) 資訊系統元件庫存清單 \| 自動化維護 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(3) | CM-8(3) 資訊系統元件庫存清單 \| 自動偵測未經授權的元件 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8(3) | CM-8(3) 資訊系統元件庫存清單 \| 自動偵測未經授權的元件 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(3) | CM-8(3) 資訊系統元件庫存清單 \| 自動偵測未經授權的元件 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-CM-8(3) | CM-8(3) 資訊系統元件庫存清單 \| 自動偵測未經授權的元件 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.A | CM-8.A 資訊系統元件庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8.A | CM-8.A 資訊系統元件庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.B | CM-8.B 資訊系統元件庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8.B | CM-8.B 資訊系統元件庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.C | CM-8.C 資訊系統元件庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8.C | CM-8.C 資訊系統元件庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.D | CM-8.D 資訊系統元件庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8.D | CM-8.D 資訊系統元件庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.E | CM-8.E 資訊系統元件庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-CM-8.E | CM-8.E 資訊系統元件庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。<br>此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) 緊急應變計畫 \| 繼續基本任務/業務職能 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2(6) | CP-2(6) 緊急應變計畫 \| 替代處理/儲存站台 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) 緊急應變計畫 \| 替代處理/儲存站台 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2(6) | CP-2(6) 緊急應變計畫 \| 替代處理/儲存站台 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) 緊急應變計畫 \| 替代處理/儲存站台 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) 緊急應變計畫 \| 替代處理/儲存站台 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) 緊急應變計畫 \| 替代處理/儲存站台 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A 緊急應變計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B 緊急應變計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C 緊急應變計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D 緊急應變計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E 緊急應變計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.R 緊急應變計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G 緊急應變計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-6(1) | CP-6(1) 替代儲存站台 \| 與主站台分離 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-6(2) | CP-6(2) 替代儲存站台 \| 復原時間/點目標 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-6.A | CP-6.A 替代儲存站台 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-6.B | CP-6.B 替代儲存站台 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。<br>此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) 資訊系統備份 \| 單獨儲存重要資訊 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| CCCS-fPBMM-CP-9(7) | CP-9(7) 資訊系統備份 \| 雙重授權 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(7) | CP-9(7) 資訊系統備份 \| 雙重授權 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-9.A | CP-9.A 資訊系統備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-9.AA | CP-9.AA 資訊系統備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-9.B | CP-9.B 資訊系統備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-9.C | CP-9.C 資訊系統備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CCCS-fPBMM-CP-9.D | CP-9.D 資訊系統備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 作業與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| CCCS-fPBMM-CP-10.A | CP-10.A 資訊系統復原與重建 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(1) | IA-2(1) 識別與驗證 (組織使用者) \| 權限帳戶的網路存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-2(1) | IA-2(1) 識別與驗證 (組織使用者) \| 權限帳戶的網路存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(1) | IA-2(1) 識別與驗證 (組織使用者) \| 權限帳戶的網路存取 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-IA-2(3) | IA-2(3) 識別與驗證 (組織使用者) \| 權限帳戶的本機存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(3) | IA-2(3) 識別與驗證 (組織使用者) \| 權限帳戶的本機存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-IA-2(3) | IA-2(3) 識別與驗證 (組織使用者) \| 權限帳戶的本機存取 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(8) | IA-2(8) 識別與驗證 (組織使用者) \| 權限帳戶的網路存取 - 阻止重播 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-2(8) | IA-2(8) 識別與驗證 (組織使用者) \| 權限帳戶的網路存取 - 阻止重播 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(8) | IA-2(8) 識別與驗證 (組織使用者) \| 權限帳戶的網路存取 - 阻止重播 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-IA-2(11) | IA-2(11) 識別與驗證 (組織使用者) \| 遠端存取 - 獨立裝置 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(11) | IA-2(11) 識別與驗證 (組織使用者) \| 遠端存取 - 獨立裝置 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-IA-2(11) | IA-2(11) 識別與驗證 (組織使用者) \| 遠端存取 - 獨立裝置 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2.A | IA-2.A 識別與驗證 (組織使用者) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2.A | IA-2.A 識別與驗證 (組織使用者) | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-2.A | IA-2.A 識別與驗證 (組織使用者) | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2.A | IA-2.A 識別與驗證 (組織使用者) | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-IA-4(4) | IA-4(4) 識別符管理 \| 識別使用者狀態 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.A | IA-4.A 識別符管理 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.A | IA-4.A 識別符管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.A | IA-4.A 識別符管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-IA-4.B | IA-4.B 識別符管理 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.B | IA-4.B 識別符管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.B | IA-4.B 識別符管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-IA-4.C | IA-4.C 識別符管理 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.C | IA-4.C 識別符管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.C | IA-4.C 識別符管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-IA-4.D | IA-4.D 識別符管理 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.D | IA-4.D 識別符管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.D | IA-4.D 識別符管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-IA-4.E | IA-4.E 識別符管理 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.E | IA-4.E 識別符管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.E | IA-4.E 識別符管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(1) | IA-5(1) 驗證器管理 \| 密碼式驗證 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(2) | IA-5(2) 驗證器管理 \| PKI 式驗證 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CCCS-fPBMM-IA-5(2) | IA-5(2) 驗證器管理 \| PKI 式驗證 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(4) | IA-5(4) 驗證器管理 \| 自動化支援密碼強度判定 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(8) | IA-5(8) 驗證器管理 \| 多重資訊系統帳戶 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-IA-5(8) | IA-5(8) 驗證器管理 \| 多重資訊系統帳戶 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(8) | IA-5(8) 驗證器管理 \| 多重資訊系統帳戶 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.A | IA-5.A 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.A | IA-5.A 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.A | IA-5.A 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.A | IA-5.A 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.B | IA-5.B 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.B | IA-5.B 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.B | IA-5.B 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.B | IA-5.B 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.C | IA-5.C 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.C | IA-5.C 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.C | IA-5.C 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.C | IA-5.C 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.D | IA-5.D 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.D | IA-5.D 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.D | IA-5.D 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.D | IA-5.D 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.E | IA-5.E 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.E | IA-5.E 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.E | IA-5.E 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.E | IA-5.E 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.F | IA-5.F 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.F | IA-5.F 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.F | IA-5.F 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.F | IA-5.F 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.G | IA-5.G 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.G | IA-5.G 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.G | IA-5.G 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.G | IA-5.G 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.H | IA-5.H 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.H | IA-5.H 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.H | IA-5.H 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.H | IA-5.H 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.I | IA-5.I 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.I | IA-5.I 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.I | IA-5.I 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.I | IA-5.I 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.J | IA-5.J 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.J | IA-5.J 驗證器管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CCCS-fPBMM-IA-5.J | IA-5.J 驗證器管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.J | IA-5.J 驗證器管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CCCS-fPBMM-IR-6(1) | IR-6(1) 事件報告 \| 自動報告 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-3.A | MA-3.A 維護工具 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-MA-3.A | MA-3.A 維護工具 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) 非本機維護 \| 稽核與檢閱 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A 媒體存取 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-RA-5.A | RA-5.A 漏洞掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-RA-5.B | RA-5.B 漏洞掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-RA-5.C | RA-5.C 漏洞掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-RA-5.D | RA-5.D 漏洞掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-RA-5.E | RA-5.E 漏洞掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SA-10(1) | SA-10(1) 開發人員組態管理 \| 軟體/韌體完整性驗證 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SC-5.A | SC-5.A 拒絕服務保護 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-5.A | SC-5.A 拒絕服務保護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流就能處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A 資源可用性 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) 邊界保護 \| 存取點 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) 邊界保障 \| 外部電信服務 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-SC-7(5) | SC-7(5) 邊界保護 \| 預設拒絕/依例外狀況允許 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(5) | SC-7(5) 邊界保護 \| 預設拒絕/依例外狀況允許 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-7(5) | SC-7(5) 邊界保護 \| 預設拒絕/依例外狀況允許 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(5) | SC-7(5) 邊界保護 \| 預設拒絕/依例外狀況允許 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-SC-7(7) | SC-7(7) 邊界保護 \| 防止遠端裝置的分割通道 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A 邊界保護 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B 邊界保護 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可防止儲存貯體層級的公開存取，有助於阻止未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C 邊界保護 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-8(1) | SC-8(1) 傳輸機密性與完整性 \| 密碼編譯或替代實體保護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8.A | SC-8.A 傳輸機密性與完整性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-12(1) | SC-12(1) 密碼編譯金鑰建立與管理 \| 可用性 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| CCCS-fPBMM-SC-12(2) | SC-12(2) 密碼編譯金鑰建立與管理 \| 對稱金鑰 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-12(2) | SC-12(2) 密碼編譯金鑰建立與管理 \| 對稱金鑰 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| CCCS-fPBMM-SC-12.A | SC-12.A 密碼編譯金鑰建立與管理 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| CCCS-fPBMM-SC-12.A | SC-12.A 密碼編譯金鑰建立與管理 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A 密碼編譯保護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-22.A | SC-22.A 名稱/位址解析服務的架構與佈建 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-23.A | SC-23.A 會話真實性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28(1) | SC-28(1) 保護靜態資訊 \| 密碼編譯保護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態的敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A 保護靜態資訊 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於發布的訊息中可能存在靜態的敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保護系統的最佳實務是安裝最新的修補程式。 |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) 修補瑕疵 \| 自動化瑕疵修補狀態 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(3) | SI-2(3) 修補瑕疵 \| 修補瑕疵的時間/更正動作基準 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保護系統的最佳實務是安裝最新的修補程式。 |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A 修補瑕疵 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保護系統的最佳實務是安裝最新的修補程式。 |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B 修補瑕疵 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保護系統的最佳實務是安裝最新的修補程式。 |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C 修補瑕疵 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保護系統的最佳實務是安裝最新的修補程式。 |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D 修補瑕疵 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| CCCS-fPBMM-SI-3(1) | SI-3(1) 惡意程式碼防護 \| 集中管理 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3(7) | SI-3(7) 惡意程式碼防護 \| 非簽章型偵測 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SI-3.A | SI-3.A 惡意程式碼防護 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.A | SI-3.A 惡意程式碼防護 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-3.A | SI-3.A 惡意程式碼防護 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.A | SI-3.A 惡意程式碼防護 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-3.A | SI-3.A 惡意程式碼防護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.B | SI-3.B 惡意程式碼防護 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-3.B | SI-3.B 惡意程式碼防護 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.B | SI-3.B 惡意程式碼防護 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-3.B | SI-3.B 惡意程式碼防護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.C | SI-3.C 惡意程式碼防護 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-3.C | SI-3.C 惡意程式碼防護 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.C | SI-3.C 惡意程式碼防護 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-3.C | SI-3.C 惡意程式碼防護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.D | SI-3.D 惡意程式碼防護 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CCCS-fPBMM-SI-3.D | SI-3.D 惡意程式碼防護 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.D | SI-3.D 惡意程式碼防護 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CCCS-fPBMM-SI-3.D | SI-3.D 惡意程式碼防護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SI-4(1) | SI-4(1) 資訊系統監控 \| 全系統入侵偵測系統 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(1) | SI-4(1) 資訊系統監控 \| 全系統入侵偵測系統 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-SI-4(2) | SI-4(2) 資訊系統監控 \| 即時分析的自動化工具 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(2) | SI-4(2) 資訊系統監控 \| 即時分析的自動化工具 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CCCS-fPBMM-SI-4(4) | SI-4(4) 資訊系統監控 \| 傳入和傳出通訊流量 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(4) | SI-4(4) 資訊系統監控 \| 傳入和傳出通訊流量 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| CCCS-fPBMM-SI-4(5) | SI-4(5) 資訊系統監控 \| 系統產生的警示 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(11) | SI-4(11) 資訊系統監控 \| 分析通訊流量異常情況 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SI-4(11) | SI-4(11) 資訊系統監控 \| 分析通訊流量異常情況 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(16) | SI-4(16) 資訊系統監控 \| 建立監控資訊關聯 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SI-4(16) | SI-4(16) 資訊系統監控 \| 建立監控資訊關聯 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(20) | SI-4(20) 資訊系統監控 \| 權限使用者 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CCCS-fPBMM-SI-4(23) | SI-4(23) 資訊系統監控 \| 主機型裝置 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(23) | SI-4(23) 資訊系統監控 \| 主機型裝置 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時，CloudTrail 將在新區域中建立相同的軌跡。因此，您將會收到包含新區域 API 活動的日誌檔，但無須採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.A | SI-4.A 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.A | SI-4.A 資訊系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-4.A | SI-4.A 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.A | SI-4.A 資訊系統監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CCCS-fPBMM-SI-4.A | SI-4.A 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.B | SI-4.B 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.B | SI-4.B 資訊系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-4.B | SI-4.B 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.B | SI-4.B 資訊系統監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CCCS-fPBMM-SI-4.B | SI-4.B 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.C | SI-4.C 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.C | SI-4.C 資訊系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-4.C | SI-4.C 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.C | SI-4.C 資訊系統監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CCCS-fPBMM-SI-4.C | SI-4.C 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.D | SI-4.D 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.D | SI-4.D 資訊系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-4.D | SI-4.D 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.D | SI-4.D 資訊系統監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CCCS-fPBMM-SI-4.D | SI-4.D 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.E | SI-4.E 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.E | SI-4.E 資訊系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-4.E | SI-4.E 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.E | SI-4.E 資訊系統監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CCCS-fPBMM-SI-4.E | SI-4.E 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.F | SI-4.F 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.F | SI-4.F 資訊系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-4.F | SI-4.F 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.F | SI-4.F 資訊系統監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CCCS-fPBMM-SI-4.F | SI-4.F 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.G | SI-4.G 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.G | SI-4.G 資訊系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-4.G | SI-4.G 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.G | SI-4.G 資訊系統監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CCCS-fPBMM-SI-4.G | SI-4.G 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-5.A | SI-5.A 安全警示、建議和指令 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SI-5.B | SI-5.B 安全警示、建議和指令 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SI-5.C | SI-5.C 安全警示、建議和指令 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-5.D | SI-5.D 安全警示、建議和指令 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CCCS-fPBMM-SI-7(1) | SI-7(1) 軟體、韌體和資訊完整性 \| 完整性檢查 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-7(7) | SI-7(7) 軟體、韌體和資訊完整性 \| 整合偵測與回應 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-7.A | SI-7.A 軟體、韌體和資訊完整性 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CCCS-fPBMM-SI-12.A | SI-12.A 資訊處理與保留 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

## 範本

範本可參閱 GitHub：加拿大網路安全中心 (CCCS) 中型雲端控制設定檔的最佳營運實務。

# 獨聯體 AWS 基金會基準 v1.4 級 1 的運營最佳實踐

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網際網路安全中心 (CIS) Amazon Web Services 基金會第 1.4 級第 1 級與 AWS 受管 Config 規則/AWS Config 程序檢查之間的範例對應。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 CIS Amazon Web Services 基金會 v1.4 級 1 控制相關。CIS Amazon Web Services Foundation v1.4 第 1 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

如需程序檢查的詳細資訊，請參閱《程序檢查》。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 維護目前的聯絡人詳細資訊 | account-contact-details-configured（過程檢查） | 確保 AWS 帳戶的聯絡人電子郵件和電話號碼是最新的，並對應至組織中的多名人員。在控制台的「我的帳戶」區段中，確保在「聯絡人資訊」區段中指定了正確的資訊。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2 | 確保已登記安全聯絡人資訊 | account-security-contact-configured (處理程序檢查) | 確保組織安全團隊的聯絡人電子郵件和電話號碼是最新的。在 AWS 管理主控台的 [我的帳戶] 區段中，確定 [安全性] 區段中已指定正確的資訊。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 1.4 | 確保不存在「根」使用者存取金鑰 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.5 | 確保已為「根」使用者啟用 MFA | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1.7 | 禁止在管理和日常任務中使用「根」使用者 | root-account-regular-use (處理程序檢查) | 確保避免在日常任務中使用根帳戶。在 IAM 中執行憑證報告，以檢查上次使用根使用者的時間。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.8 | 確保 IAM 密碼政策的長度至少在 14 個字元以上 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.9 | 確保 IAM 密碼政策防止重複使用密碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.10 | 確保擁有主控台密碼的所有使用者皆已啟用多重要素驗證 (MFA) | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.11 | 不要在初次進行使用者設定時，為擁有主控台密碼的所有使用者設定存取金鑰 | Iam-用戶控制台和-（過程檢查）api-access-at-creation | 確保不要在初次進行使用者設定時，為擁有主控台密碼的所有使用者設定存取金鑰。對於具有主控台存取權限的所有使用者，請將使用者的「建立時間」與存取金鑰「建立」日期進行比較。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.12 | 確保停用 45 天 (含) 以上未使用的憑證 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將 maxCredentialUsage 年齡值設定為 (CIS 標準值：45)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.13 | 確保任何單一使用者只能使用一個作用中的存取金鑰 | iam-user-single-access-key (處理程序檢查) | 確保任何單一使用者只能使用一個作用中的存取金鑰。請針對所有使用者檢查 IAM 中每個使用者的「安全登入資料」索引標籤中是否只使用一個作用中金鑰。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 1.14 | 確保在每 90 天或更短的期限內輪換存取金鑰 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.15 | 確保使用者僅透過群組接收許可 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 1.15 | 確保使用者僅透過群組接收許可 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 1.15 | 確保使用者僅透過群組接收許可 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.16 | 確保並未連接允許完整 "*:*" 管理權限的 IAM 政策 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 1.17 | 透過 Support，確保已建立支 AWS 援角色來管理事件 | iam-policy-in-use | AWS Identity and Access Management (IAM) 可確保將 IAM 政策指派給適當的使用者、角色或群組，協助您管理存取許可和授權。限制這些政策也會整合最低權限和職責分離的原則。此規則需要您將政策紗線設定為 arn: aw:iam:: aw:aw: 政策/，以便使用 Support 進行事件管理。AWSSupportAccess AWS |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.19 | 請確保刪除儲存在 AWS IAM 中的所有過期 SSL/TLS 憑證 | iam-expired-certificates (處理程序檢查) | 請確保刪除儲存在 IAM 中的所有過期 SSL/TLS 憑證。從帶有已安裝 AWS CLI 的命令行中運行「AWS iam list-server-certificates」命令，並確定是否有任何過期的服務器證書。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.20 | 確保 AWS IAM 存取分析器已啟用 | iam-access-analyzer-enabled (處理程序檢查) | 確保已啟用 IAM Access Analyzer。在主控台的 IAM 區段中，選取「存取分析器」，並確定「狀態」設定為「作用中」。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1.3 | 確保 S3 儲存貯體已啟用 MFA 刪除功能 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。為 S3 儲存貯體新增多重要素驗證 (MFA) 刪除，需要額外的驗證因素才能變更儲存貯體的版本狀態或刪除物件版本。MFA 刪除可以在安全憑證遭到入侵或授予未經授權存取的情況下增加一層額外的安全性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1.5 | 確保 S3 儲存貯體設定為「封鎖公開存取 (儲存貯體設定)」 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 2.1.5 | 確保 S3 儲存貯體設定為「封鎖公開存取 (儲存貯體設定)」 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.1 | 確保已啟用 EBS 磁碟區加密 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 2.2.1 | 確保已啟用 EBS 磁碟區加密 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.3.1 | 確保已啟用 RDS 執行個體的加密 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.3.1 | 確保已啟用 RDS 執行個體的加密 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.1 | 確保 CloudTrail 在所有區域都啟用 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.3 | 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.3 | 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 確保跟 CloudTrail 踪與 CloudWatch日誌集成 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 3.6 | 確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取日誌 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示 | alarm-unauthorized-api-calls (處理程序檢查) | 確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.2 | 確保不使用 MFA 的管理主控台登入存在日誌指標篩選條件和警示 | 報警-sign-in-without-mfa （過程檢查） | 確定不使用多重要素驗證 (MFA) 的 AWS 管理主控台登入存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.3 | 確保「根」帳戶的使用存在日誌指標篩選條件和警示 | alarm-root-account-use (處理程序檢查) | 確保根帳戶的使用存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.4 | 確保 IAM 政策變更存在日誌指標篩選條件和警示 | alarm-iam-policy-change (處理程序檢查) | 確保 IAM 政策變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.5 | 確保存在 CloudTrail配置更改的日誌指標過濾器和警報 | alarm-cloudtrail-config-change (處理程序檢查) | 確保存有日誌指標過濾器和 AWS CloudTrail 配置更改的警報。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.8 | 確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示 | 警報 -3-bucket-policy-change (程序檢查) | 確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.12 | 確保網路閘道變更存在日誌指標篩選條件和警示 | 報警-vpc-network-gateway-change（過程檢查） | 確保網路閘道變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.13 | 確保路由表變更存在日誌指標篩選條件和警示 | 報警-vpc-route-table-change（過程檢查） | 確保路由表變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.14 | 確保 VPC 變更存在日誌指標篩選條件和警示 | alarm-vpc-change (處理程序檢查) | 確保 Amazon 虛擬私有雲端 (VPC) 變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.15 | 確保 AWS Organizations變更存在日誌指標篩選條件和警示 | alarm-organizations-change (處理程序檢查) | 確保 AWS Organizations 變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.1 | 確保沒有網路 ACL 允許從 0.0.0.0/0 傳入至遠端伺服器管理連接埠的流量 | nacl-no-unrestricted-ssh-rdp | 確保沒有任何網路 ACL 允許公用流量輸入至遠端伺服器管理連接埠。在主控台的 VPC 區段中，確定具有來源為「0.0.0.0/0」的網路 ACL，並具備允許的連接埠或連接埠範圍，包括遠端伺服器管理連接埠。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 5.2 | 確保沒有安全群組允許流量從 0.0.0.0/0 輸入至遠端伺服器管理連接埠 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 確保沒有安全群組允許流量從 0.0.0.0/0 輸入至遠端伺服器管理連接埠 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則允許您選擇性地設定 blockedPort1 - blockedPort5 參數 (CIS 標準值：3389)。實際值應反映貴組織的政策。 |

### 範本

該模板可用於 GitHub：CIS AWS 基準基準 v1.4 級 1 的運營最佳實踐。

## 獨聯體 AWS 基金會基準第 1.4 版第 2 級的運營最佳實踐

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網際網路安全中心 (CIS) Amazon Web Services 基金會第 1.4 級第 2 級與 AWS 受管 Config 規則/AWS Config 程序檢查之間的範例對應。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 CIS Amazon Web Services 基金會 v1.4 第 2 級控制相關。CIS Amazon Web Services Foundation v1.4 第 2 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

如需程序檢查的詳細資訊，請參閱《程序檢查》。

AWS 區域：所有支援一致性套件的地 AWS 區域 方 (區域支援)，但 AWS GovCloud (美國東部)、AWS GovCloud (美國西部) 及中東 (巴林) 除外

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 維護目前的聯絡人詳細資訊 | account-contact-details-configured（過程檢查） | 確保 AWS 帳戶的聯絡人電子郵件和電話號碼是最新的，並對應至組織中的多名人員。在控制台的「我的帳戶」區段中，確保在「聯絡人資訊」區段中指定了正確的資訊。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 1.2 | 確保已登記安全聯絡人資訊 | account-security-contact-configured (處理程序檢查) | 確保組織安全團隊的聯絡人電子郵件和電話號碼是最新的。在 AWS 管理主控台的 [我的帳戶] 區段中，確定 [安全性] 區段中已指定正確的資訊。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 1.4 | 確保不存在「根」使用者存取金鑰 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 1.5 | 確保已為「根」使用者啟用 MFA | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.6 | 確保「根」使用者帳戶已啟用硬體 MFA | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1.7 | 禁止在管理和日常任務中使用「根」使用者 | root-account-regular-use (處理程序檢查) | 確保避免在日常任務中使用根帳戶。在 IAM 中執行憑證報告，以檢查上次使用根使用者的時間。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.8 | 確保 IAM 密碼政策的長度至少在 14 個字元以上 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.9 | 確保 IAM 密碼政策防止重複使用密碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.10 | 確保擁有主控台密碼的所有使用者皆已啟用多重要素驗證 (MFA) | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.11 | 不要在初次進行使用者設定時，為擁有主控台密碼的所有使用者設定存取金鑰 | Iam-用戶控制台和-（過程檢查）api-access-at-creation | 確保不要在初次進行使用者設定時，為擁有主控台密碼的所有使用者設定存取金鑰。對於具有主控台存取權限的所有使用者，請將使用者的「建立時間」與存取金鑰「建立」日期進行比較。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.12 | 確保停用 45 天 (含) 以上未使用的憑證 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將 maxCredentialUsage 年齡值設定為 (CIS 標準值：45)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.13 | 確保任何單一使用者只能使用一個作用中的存取金鑰 | iam-user-single-access-key (處理程序檢查) | 確保任何單一使用者只能使用一個作用中的存取金鑰。請針對所有使用者檢查 IAM 中每個使用者的「安全登入資料」索引標籤中是否只使用一個作用中金鑰。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 1.14 | 確保在每 90 天或更短的期限內輪換存取金鑰 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.15 | 確保使用者僅透過群組接收許可 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 1.15 | 確保使用者僅透過群組接收許可 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 1.15 | 確保使用者僅透過群組接收許可 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.16 | 確保並未連接允許完整 "*:*" 管理權限的 IAM 政策 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 1.17 | 透過 Support，確保已建立支 AWS 援角色來管理事件 | iam-policy-in-use | AWS Identity and Access Management (IAM) 可確保將 IAM 政策指派給適當的使用者、角色或群組，協助您管理存取許可和授權。限制這些政策也會整合最低權限和職責分離的原則。此規則需要您將政策紗線設定為 arn: aw:iam:: aw:aw: 政策/，以便使用 Support 進行事件管理。AWSSupportAccess AWS |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.18 | 確保 IAM 執行個體角色用於從執行個體存取 AWS 資源 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 1.19 | 請確保刪除儲存在 AWS IAM 中的所有過期 SSL/TLS 憑證 | iam-expired-certificates (處理程序檢查) | 請確保刪除儲存在 IAM 中的所有過期 SSL/TLS 憑證。從已安裝 AWS CLI 的命令行中運行 'AWS iam list-server-certificates' 命令，並確定是否有任何過期的服務器證書。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.20 | 確保 AWS IAM 存取分析器已啟用 | iam-access-analyzer-enabled (處理程序檢查) | 確保已啟用 IAM Access Analyzer。在主控台的 IAM 區段中，選取「存取分析器」，並確定「狀態」設定為「作用中」。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 1.21 | 確保透過身分識別同盟集中管理使用者或多帳戶環境的 Organ AWS izations | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1.1 | 確保使用所有 S3 儲存貯體 encryption-at-rest | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 2.1.2 | 確保 S3 儲存貯體政策設定為拒絕 HTTP 請求 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1.3 | 確保 S3 儲存貯體已啟用 MFA 刪除功能 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。為 S3 儲存貯體新增多重要素驗證 (MFA) 刪除，需要額外的驗證因素才能變更儲存貯體的版本狀態或刪除物件版本。MFA 刪除可以在安全憑證遭到入侵或授予未經授權存取的情況下增加一層額外的安全性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1.5 | 確保 S3 儲存貯體設定為「封鎖公開存取 (儲存貯體設定)」 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 2.1.5 | 確保 S3 儲存貯體設定為「封鎖公開存取 (儲存貯體設定)」 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.1 | 確保已啟用 EBS 磁碟區加密 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 2.2.1 | 確保已啟用 EBS 磁碟區加密 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.3.1 | 確保已啟用 RDS 執行個體的加密 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.3.1 | 確保已啟用 RDS 執行個體的加密 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.1 | 確保 CloudTrail 在所有區域都啟用 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2 | 確定已啟用 CloudTrail 記錄檔驗證 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 3.3 | 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.3 | 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 3.4 | 確保跟 CloudTrail 踪與 CloudWatch日誌集成 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5 | 確保所有區域都啟用了 AWS Config | config-enabled-all-regions (處理程序檢查) | 確保在所有 AWS 區域中啟用 AWS Config。在控制台的 AWS Config 部分中，對於每個啟用的區域，請確保 Con AWS fig 記錄器正確配置。確保至少在一個區域中啟用全域 AWS 資源的記錄功能。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6 | 確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取日誌 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.7 | 確保使用 KMS CMK 在靜態時加密 CloudTrail 記錄 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| 3.8 | 確保為客戶建立的 CMK 啟用輪換功能 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.9 | 確保所有 VPC 中皆已啟用 VPC 流程日誌記錄 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 3.10 | 確保已為 S3 儲存貯體啟用寫入事件的物件層級日誌記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 3.11 | 確保已為 S3 儲存貯體啟用讀取事件的物件層級日誌記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示 | alarm-unauthorized-api-calls (處理程序檢查) | 確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.2 | 確保不使用 MFA 的管理主控台登入存在日誌指標篩選條件和警示 | 報警-sign-in-without-mfa （過程檢查） | 確定不使用多重要素驗證 (MFA) 的 AWS 管理主控台登入存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.3 | 確保「根」帳戶的使用存在日誌指標篩選條件和警示 | alarm-root-account-use (處理程序檢查) | 確保根帳戶的使用存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.4 | 確保 IAM 政策變更存在日誌指標篩選條件和警示 | alarm-iam-policy-change (處理程序檢查) | 確保 IAM 政策變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.5 | 確保存在 CloudTrail配置更改的日誌指標過濾器和警報 | alarm-cloudtrail-config-change (處理程序檢查) | 確保存有日誌指標過濾器和 AWS CloudTrail 配置更改的警報。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.6 | 確保 AWS 管理主控台身分驗證失敗存在日誌指標篩選條件和警示 | alarm-console-auth-failures (處理程序檢查) | 確保 AWS 管理主控台身分驗證失敗存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.7 | 確保停用或排定刪除客戶建立的 CMK 存在日誌指標篩選條件和警示 | 警報公里-disable-or-delete-cmk（過程檢查） | 確保停用或排定刪除客戶建立的 CMK 存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.8 | 確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示 | 警報 -3-bucket-policy-change (程序檢查) | 確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.9 | 確保 Con AWS fig 配置更改存在日誌指標過濾器和警報 | alarm-aws-config-change (處理程序檢查) | 確保 AWS Config 組態變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.10 | 確保安全群組變更存在日誌指標篩選條件和警示 | 報警-vpc-secrity-group-change（過程檢查） | 確保安全群組變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.11 | 確保網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示 | alarm-vpc-nacl-change (處理程序檢查) | 確保網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.12 | 確保網路閘道變更存在日誌指標篩選條件和警示 | 報警-vpc-network-gateway-change（過程檢查） | 確保網路閘道變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.13 | 確保路由表變更存在日誌指標篩選條件和警示 | 報警-vpc-route-table-change（過程檢查） | 確保路由表變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 4.14 | 確保 VPC 變更存在日誌指標篩選條件和警示 | alarm-vpc-change (處理程序檢查) | 確保 Amazon 虛擬私有雲端 (VPC) 變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.15 | 確保 AWS Organizations變更存在日誌指標篩選條件和警示 | alarm-organizations-change (處理程序檢查) | 確保 AWS Organizations 變更存在日誌指標篩選條件和警示。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.1 | 確保沒有網路 ACL 允許從 0.0.0.0/0 傳入至遠端伺服器管理連接埠的流量 | nacl-no-unrestricted-ssh-rdp | 確保沒有任何網路 ACL 允許公用流量輸入至遠端伺服器管理連接埠。在主控台的 VPC 區段中，確定具有來源為「0.0.0.0/0」的網路 ACL，並具備允許的連接埠或連接埠範圍，包括遠端伺服器管理連接埠。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |
| 5.2 | 確保沒有安全群組允許流量從 0.0.0.0/0 輸入至遠端伺服器管理連接埠 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 確保沒有安全群組允許流量從 0.0.0.0/0 輸入至遠端伺服器管理連接埠 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則允許您選擇性地設定 blockedPort1 - blockedPort5 參數 (CIS 標準值：3389)。實際值應反映貴組織的政策。 |
| 5.3 | 確保每個 VPC 的預設安全群組都會限制所有流量 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4 | 確保 VPC 對等路由表為「最低權限」 | vpc-peering-least-access (處理程序檢查) | 確保 Amazon VPC 對等路由表為「最低權限」。在主控台的 VPC 區段中，檢查路由表項目，以確保完成對等互連目的所需的最少子網路或主機數量是可路由的。如需此控制之稽核的進一步詳細資訊，請參閱《CIS Amazon Web Services Foundations 基準版本 1.4.0》文件，網址為 https://www.cisecurity.org/benchmark/amazon_web_services/ |

### 範本

該模板可用於 GitHub：CIS AWS 基準基準 v1.4 級 2 的運營最佳實踐。

## CIS Critical Security Controls v8 IG1 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網際網路安全中心 (CIS) 關鍵安全控制 v8 IG1 與 AWS 受管 Config 規則之間的對應範例。每個都 AWS Config 適用於特定 AWS 資源，並與一個或多個 CIS 關鍵安全控制 v8 IG1 控制項相關。一個 CIS Critical Security Controls v8 IG1 控制項可以與多個 AWS Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-security-group-attached-to-eni | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控庫存清單中未使用的安全群組並管理您的環境。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 確保目前支援授權的軟體 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 2.2 | 確保目前支援授權的軟體 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 確保目前支援授權的軟體 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| 3.3 | 設定資料存取控制清單 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 3.3 | 設定資料存取控制清單 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.3 | 設定資料存取控制清單 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.3 | 設定資料存取控制清單 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或任務職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制與復原，以及委派許可管理功能。 |
| 3.3 | 設定資料存取控制清單 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.3 | 設定資料存取控制清單 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.3 | 設定資料存取控制清單 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3.3 | 設定資料存取控制清單 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.3 | 設定資料存取控制清單 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 3.3 | 設定資料存取控制清單 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 3.3 | 設定資料存取控制清單 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 3.3 | 設定資料存取控制清單 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.3 | 設定資料存取控制清單 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.3 | 設定資料存取控制清單 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.3 | 設定資料存取控制清單 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.3 | 設定資料存取控制清單 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.3 | 設定資料存取控制清單 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.3 | 設定資料存取控制清單 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 3.3 | 設定資料存取控制清單 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| 3.3 | 設定資料存取控制清單 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.3 | 設定資料存取控制清單 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 3.4 | 強制執行資料保留 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 強制執行資料保留 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 4.1 | 建立並維護安全的組態程序 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 4.1 | 建立並維護安全的組態程序 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| 4.1 | 建立並維護安全的組態程序 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 4.1 | 建立並維護安全的組態程序 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 4.1 | 建立並維護安全的組態程序 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 4.1 | 建立並維護安全的組態程序 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.6 | 安全地管理企業資產和軟體 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 4.6 | 安全地管理企業資產和軟體 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.6 | 安全地管理企業資產和軟體 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 4.7 | 管理企業資產和軟體的預設帳戶 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.1 | 建立和維護帳戶庫存清單 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 5.2 | 使用唯一密碼 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 5.3 | 停用休眠帳戶 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4 | 限制專用管理員帳戶的管理員權限 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 5.4 | 限制專用管理員帳戶的管理員權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 6.5 | 需要 MFA 才能進行管理存取 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 7.1 | 建立並維護漏洞管理程序 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1 | 建立並維護漏洞管理程序 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 7.1 | 建立並維護漏洞管理程序 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.3 | 執行自動化作業系統修補管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 7.3 | 執行自動化作業系統修補管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.3 | 執行自動化作業系統修補管理 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 7.4 | 執行自動化應用程式修補管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.4 | 執行自動化應用程式修補管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 7.4 | 執行自動化應用程式修補管理 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | 建立並維護稽核日誌管理程序 | audit-log-policy-exists（過程檢查） | 建立並維護稽核日誌管理政策，以定義組織的日誌記錄要求。這包括但不限於檢閱和保留稽核日誌。 |
| 8.2 | 收集稽核日誌 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 8.2 | 收集稽核日誌 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 8.2 | 收集稽核日誌 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 8.2 | 收集稽核日誌 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 8.2 | 收集稽核日誌 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 8.2 | 收集稽核日誌 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 8.2 | 收集稽核日誌 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 8.2 | 收集稽核日誌 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 8.3 | 確保進行適當的稽核日誌儲存 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 10.1 | 部署和維護反惡意軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2 | 設定自動反惡意軟體簽章更新 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 11.2 | 執行自動備份 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| 11.2 | 執行自動備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 11.2 | 執行自動備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 11.2 | 執行自動備份 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 11.2 | 執行自動備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 11.2 | 執行自動備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 11.3 | 保護復原資料 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 保護復原資料 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 11.3 | 保護復原資料 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 保護復原資料 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表過去 35 天的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

### 範本

該模板可用於 GitHub：CIS 關鍵安全控制 v8 IG1 的操作最佳實踐。

## CIS Critical Security Controls v8 IG2 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網際網路安全中心 (CIS) 關鍵安全控制 v8 IG2 與 AWS 託管 Config 規則之間的對應範例。每個都 AWS Config 適用於特定 AWS 資源，並與一個或多個 CIS 關鍵安全控制 v8 IG2 控制項相關。一個 CIS Critical Security Controls v8 IG2 控制可以與多個 AWS Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-security-group-attached-to-eni | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控庫存清單中未使用的安全群組並管理您的環境。 |
| 2.2 | 確保目前支援授權的軟體 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 2.2 | 確保目前支援授權的軟體 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 確保目前支援授權的軟體 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| 2.4 | 利用自動化軟體清查工具 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.4 | 利用自動化軟體清查工具 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 3.3 | 設定資料存取控制清單 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |
| 3.3 | 設定資料存取控制清單 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.3 | 設定資料存取控制清單 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.3 | 設定資料存取控制清單 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或任務職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制與復原，以及委派許可管理功能。 |
| 3.3 | 設定資料存取控制清單 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.3 | 設定資料存取控制清單 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.3 | 設定資料存取控制清單 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3.3 | 設定資料存取控制清單 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.3 | 設定資料存取控制清單 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 3.3 | 設定資料存取控制清單 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 3.3 | 設定資料存取控制清單 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 3.3 | 設定資料存取控制清單 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.3 | 設定資料存取控制清單 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.3 | 設定資料存取控制清單 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.3 | 設定資料存取控制清單 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.3 | 設定資料存取控制清單 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.3 | 設定資料存取控制清單 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.3 | 設定資料存取控制清單 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 3.3 | 設定資料存取控制清單 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| 3.3 | 設定資料存取控制清單 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.3 | 設定資料存取控制清單 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 3.4 | 強制執行資料保留 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 強制執行資料保留 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 3.10 | 加密傳輸中的敏感資料 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 3.10 | 加密傳輸中的敏感資料 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.10 | 加密傳輸中的敏感資料 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.10 | 加密傳輸中的敏感資料 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.10 | 加密傳輸中的敏感資料 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.10 | 加密傳輸中的敏感資料 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.10 | 加密傳輸中的敏感資料 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.10 | 加密傳輸中的敏感資料 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.10 | 加密傳輸中的敏感資料 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.10 | 加密傳輸中的敏感資料 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 3.11 | 加密靜態敏感資料 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 3.11 | 加密靜態敏感資料 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 3.11 | 加密靜態敏感資料 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 3.11 | 加密靜態敏感資料 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 3.11 | 加密靜態敏感資料 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 3.11 | 加密靜態敏感資料 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 4.1 | 建立並維護安全的組態程序 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 4.1 | 建立並維護安全的組態程序 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 4.1 | 建立並維護安全的組態程序 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 4.1 | 建立並維護安全的組態程序 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 4.1 | 建立並維護安全的組態程序 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.6 | 安全地管理企業資產和軟體 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 4.6 | 安全地管理企業資產和軟體 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.6 | 安全地管理企業資產和軟體 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 4.7 | 管理企業資產和軟體的預設帳戶 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.1 | 建立和維護帳戶庫存清單 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 5.2 | 使用唯一密碼 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 5.3 | 停用休眠帳戶 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4 | 限制專用管理員帳戶的管理員權限 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 5.4 | 限制專用管理員帳戶的管理員權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 5.6 | 集中管理帳戶 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 6.5 | 需要 MFA 才能進行管理存取 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 6.7 | 集中管理存取控制 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1 | 建立並維護漏洞管理程序 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 7.1 | 建立並維護漏洞管理程序 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1 | 建立並維護漏洞管理程序 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 7.3 | 執行自動化作業系統修補管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 7.3 | 執行自動化作業系統修補管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.3 | 執行自動化作業系統修補管理 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 7.4 | 執行自動化應用程式修補管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.4 | 執行自動化應用程式修補管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 7.4 | 執行自動化應用程式修補管理 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.5 | 對內部企業資產執行自動化漏洞掃瞄 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存映像的完整性和安全性新增一層驗證。 |
| 8.1 | 建立並維護稽核日誌管理程序 | audit-log-policy-exists（過程檢查） | 建立並維護稽核日誌管理政策，以定義組織的日誌記錄要求。這包括但不限於檢閱和保留稽核日誌。 |
| 8.2 | 收集稽核日誌 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 8.2 | 收集稽核日誌 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 8.2 | 收集稽核日誌 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 8.2 | 收集稽核日誌 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 8.2 | 收集稽核日誌 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 8.2 | 收集稽核日誌 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 8.2 | 收集稽核日誌 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 8.3 | 確保進行適當的稽核日誌儲存 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 8.5 | 收集詳細的稽核日誌 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 8.5 | 收集詳細的稽核日誌 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 8.5 | 收集詳細的稽核日誌 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 8.5 | 收集詳細的稽核日誌 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 8.5 | 收集詳細的稽核日誌 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 8.5 | 收集詳細的稽核日誌 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 8.5 | 收集詳細的稽核日誌 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 8.5 | 收集詳細的稽核日誌 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 8.7 | 收集 URL 請求稽核日誌 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.9 | 集中管理稽核日誌 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 8.10 | 保留稽核日誌 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 8.10 | 保留稽核日誌 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 10.1 | 部署和維護反惡意軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2 | 設定自動反惡意軟體簽章更新 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 10.4 | 設定抽取式媒體的自動反惡意軟體掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 10.6 | 集中管理反惡意軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.7 | 使用行為型反惡意軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 11.2 | 執行自動備份 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| 11.2 | 執行自動備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 11.2 | 執行自動備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 11.2 | 執行自動備份 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 11.2 | 執行自動備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 11.2 | 執行自動備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 11.3 | 保護復原資料 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 保護復原資料 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 11.3 | 保護復原資料 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 保護復原資料 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表過去 35 天的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 12.2 | 建立並維護安全的網路架構 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 12.2 | 建立並維護安全的網路架構 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 12.2 | 建立並維護安全的網路架構 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 12.2 | 建立並維護安全的網路架構 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 12.2 | 建立並維護安全的網路架構 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 12.2 | 建立並維護安全的網路架構 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 12.2 | 建立並維護安全的網路架構 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 12.2 | 建立並維護安全的網路架構 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。阻止直接存取網際網路可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 12.2 | 建立並維護安全的網路架構 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 12.2 | 建立並維護安全的網路架構 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 12.2 | 建立並維護安全的網路架構 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 12.2 | 建立並維護安全的網路架構 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 12.2 | 建立並維護安全的網路架構 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 12.2 | 建立並維護安全的網路架構 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| 12.3 | 安全地管理網路基礎設施 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 12.3 | 安全地管理網路基礎設施 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.3 | 安全地管理網路基礎設施 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 12.3 | 安全地管理網路基礎設施 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.3 | 安全地管理網路基礎設施 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.3 | 安全地管理網路基礎設施 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.3 | 安全地管理網路基礎設施 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 12.3 | 安全地管理網路基礎設施 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 12.6 | 使用安全的網路管理和通訊協定 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.6 | 使用安全的網路管理和通訊協定 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.6 | 使用安全的網路管理和通訊協定 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 12.6 | 使用安全的網路管理和通訊協定 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.6 | 使用安全的網路管理和通訊協定 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.6 | 使用安全的網路管理和通訊協定 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.6 | 使用安全的網路管理和通訊協定 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.6 | 使用安全的網路管理和通訊協定 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 13.1 | 集中管理安全事件提醒 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 13.1 | 集中管理安全事件提醒 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 13.3 | 部署網路入侵偵測解決方案 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 13.6 | 收集網路流量流程日誌 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 13.6 | 收集網路流量流程日誌 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

### 範本

該模板可用於 GitHub：CIS 關鍵安全控制 v8 IG2 的操作最佳實踐。

## CIS Critical Security Controls v8 IG3 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網際網路安全中心 (CIS) 關鍵安全控制 v8 IG3 與 AWS 託管 Config 規則之間的對應範例。每個都 AWS Config 適用於特定 AWS 資源，並與一個或多個 CIS 關鍵安全控制 v8 IG3 控制項相關。一個 CIS Critical Security Controls v8 IG3 控制可以與多個 AWS Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | eip-attached | 此規則可確保配置給 Amazon Virtual |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.1 | 建立並維護詳細的企業資產庫存清單 | ec2-security-group-attached-to-eni | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控庫存清單中未使用的安全群組並管理您的環境。 |
| 2.2 | 確保目前支援授權的軟體 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 2.2 | 確保目前支援授權的軟體 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 確保目前支援授權的軟體 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| 2.4 | 利用自動化軟體清查工具 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.4 | 利用自動化軟體清查工具 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| 3.3 | 設定資料存取控制清單 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |
| 3.3 | 設定資料存取控制清單 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.3 | 設定資料存取控制清單 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.3 | 設定資料存取控制清單 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或任務職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制與復原，以及委派許可管理功能。 |
| 3.3 | 設定資料存取控制清單 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.3 | 設定資料存取控制清單 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.3 | 設定資料存取控制清單 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3.3 | 設定資料存取控制清單 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.3 | 設定資料存取控制清單 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 3.3 | 設定資料存取控制清單 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 3.3 | 設定資料存取控制清單 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 3.3 | 設定資料存取控制清單 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.3 | 設定資料存取控制清單 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.3 | 設定資料存取控制清單 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.3 | 設定資料存取控制清單 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.3 | 設定資料存取控制清單 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.3 | 設定資料存取控制清單 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.3 | 設定資料存取控制清單 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 3.3 | 設定資料存取控制清單 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| 3.3 | 設定資料存取控制清單 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 設定資料存取控制清單 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.3 | 設定資料存取控制清單 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 3.4 | 強制執行資料保留 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 強制執行資料保留 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 3.10 | 加密傳輸中的敏感資料 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 3.10 | 加密傳輸中的敏感資料 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.10 | 加密傳輸中的敏感資料 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.10 | 加密傳輸中的敏感資料 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.10 | 加密傳輸中的敏感資料 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.10 | 加密傳輸中的敏感資料 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.10 | 加密傳輸中的敏感資料 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.10 | 加密傳輸中的敏感資料 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.10 | 加密傳輸中的敏感資料 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.10 | 加密傳輸中的敏感資料 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 3.11 | 加密靜態敏感資料 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 3.11 | 加密靜態敏感資料 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 3.11 | 加密靜態敏感資料 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 3.11 | 加密靜態敏感資料 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 3.11 | 加密靜態敏感資料 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11 | 加密靜態敏感資料 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.11 | 加密靜態敏感資料 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 3.11 | 加密靜態敏感資料 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14 | 記錄敏感資料存取 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.14 | 記錄敏感資料存取 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 3.14 | 記錄敏感資料存取 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14 | 記錄敏感資料存取 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.14 | 記錄敏感資料存取 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 3.14 | 記錄敏感資料存取 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14 | 記錄敏感資料存取 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 3.14 | 記錄敏感資料存取 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 3.14 | 記錄敏感資料存取 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14 | 記錄敏感資料存取 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14 | 記錄敏感資料存取 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 3.14 | 記錄敏感資料存取 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14 | 記錄敏感資料存取 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.14 | 記錄敏感資料存取 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 4.1 | 建立並維護安全的組態程序 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 4.1 | 建立並維護安全的組態程序 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 4.1 | 建立並維護安全的組態程序 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 建立並維護安全的組態程序 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 4.1 | 建立並維護安全的組態程序 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 4.1 | 建立並維護安全的組態程序 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.6 | 安全地管理企業資產和軟體 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 4.6 | 安全地管理企業資產和軟體 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.6 | 安全地管理企業資產和軟體 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4.6 | 安全地管理企業資產和軟體 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 4.7 | 管理企業資產和軟體的預設帳戶 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.1 | 建立和維護帳戶庫存清單 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 5.2 | 使用唯一密碼 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 使用唯一密碼 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 5.3 | 停用休眠帳戶 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4 | 限制專用管理員帳戶的管理員權限 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 5.4 | 限制專用管理員帳戶的管理員權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 5.6 | 集中管理帳戶 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.4 | 需要 MFA 才能進行遠端網路存取 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 6.5 | 需要 MFA 才能進行管理存取 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 6.7 | 集中管理存取控制 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1 | 建立並維護漏洞管理程序 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 7.1 | 建立並維護漏洞管理程序 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1 | 建立並維護漏洞管理程序 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 7.3 | 執行自動化作業系統修補管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 7.3 | 執行自動化作業系統修補管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.3 | 執行自動化作業系統修補管理 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 7.4 | 執行自動化應用程式修補管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.4 | 執行自動化應用程式修補管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 7.4 | 執行自動化應用程式修補管理 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.5 | 對內部企業資產執行自動化漏洞掃瞄 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存映像的完整性和安全性新增一層驗證。 |
| 8.1 | 建立並維護稽核日誌管理程序 | audit-log-policy-exists（過程檢查） | 建立並維護稽核日誌管理政策，以定義組織的日誌記錄要求。這包括但不限於檢閱和保留稽核日誌。 |
| 8.2 | 收集稽核日誌 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 8.2 | 收集稽核日誌 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 8.2 | 收集稽核日誌 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 8.2 | 收集稽核日誌 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 8.2 | 收集稽核日誌 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 8.2 | 收集稽核日誌 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 8.2 | 收集稽核日誌 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2 | 收集稽核日誌 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 8.3 | 確保進行適當的稽核日誌儲存 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 8.5 | 收集詳細的稽核日誌 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 8.5 | 收集詳細的稽核日誌 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 8.5 | 收集詳細的稽核日誌 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 8.5 | 收集詳細的稽核日誌 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 8.5 | 收集詳細的稽核日誌 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 8.5 | 收集詳細的稽核日誌 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 8.5 | 收集詳細的稽核日誌 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.5 | 收集詳細的稽核日誌 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 8.5 | 收集詳細的稽核日誌 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 8.7 | 收集 URL 請求稽核日誌 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.9 | 集中管理稽核日誌 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 8.10 | 保留稽核日誌 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 8.10 | 保留稽核日誌 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 10.1 | 部署和維護反惡意軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2 | 設定自動反惡意軟體簽章更新 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 10.4 | 設定抽取式媒體的自動反惡意軟體掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 10.6 | 集中管理反惡意軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.7 | 使用行為型反惡意軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 11.2 | 執行自動備份 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| 11.2 | 執行自動備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 11.2 | 執行自動備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 11.2 | 執行自動備份 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 11.2 | 執行自動備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 11.2 | 執行自動備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | 執行自動備份 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 11.3 | 保護復原資料 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 保護復原資料 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 11.3 | 保護復原資料 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 保護復原資料 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表過去 35 天的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 建立並維護隔離的復原資料執行個體 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 12.2 | 建立並維護安全的網路架構 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 12.2 | 建立並維護安全的網路架構 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 12.2 | 建立並維護安全的網路架構 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 12.2 | 建立並維護安全的網路架構 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 12.2 | 建立並維護安全的網路架構 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 12.2 | 建立並維護安全的網路架構 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 12.2 | 建立並維護安全的網路架構 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 12.2 | 建立並維護安全的網路架構 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 12.2 | 建立並維護安全的網路架構 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。阻止直接存取網際網路可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 12.2 | 建立並維護安全的網路架構 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 12.2 | 建立並維護安全的網路架構 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 12.2 | 建立並維護安全的網路架構 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 12.2 | 建立並維護安全的網路架構 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 12.2 | 建立並維護安全的網路架構 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 12.2 | 建立並維護安全的網路架構 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.2 | 建立並維護安全的網路架構 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| 12.3 | 安全地管理網路基礎設施 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 12.3 | 安全地管理網路基礎設施 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.3 | 安全地管理網路基礎設施 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 12.3 | 安全地管理網路基礎設施 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.3 | 安全地管理網路基礎設施 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.3 | 安全地管理網路基礎設施 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.3 | 安全地管理網路基礎設施 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 12.3 | 安全地管理網路基礎設施 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 12.6 | 使用安全的網路管理和通訊協定 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.6 | 使用安全的網路管理和通訊協定 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.6 | 使用安全的網路管理和通訊協定 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 12.6 | 使用安全的網路管理和通訊協定 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.6 | 使用安全的網路管理和通訊協定 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.6 | 使用安全的網路管理和通訊協定 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 12.6 | 使用安全的網路管理和通訊協定 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.6 | 使用安全的網路管理和通訊協定 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 13.1 | 集中管理安全事件提醒 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 13.1 | 集中管理安全事件提醒 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 13.3 | 部署網路入侵偵測解決方案 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 13.6 | 收集網路流量流程日誌 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 13.6 | 收集網路流量流程日誌 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 13.10 | 執行應用程式層篩選 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_SECRE T_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| 16.1 | 建立並維護安全的應用程式開發程序 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16.12 | 實作程式碼層級安全檢查 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 16.12 | 實作程式碼層級安全檢查 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 16.12 | 實作程式碼層級安全檢查 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16.12 | 實作程式碼層級安全檢查 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| 16.12 | 實作程式碼層級安全檢查 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

### 範本

該模板可用於 GitHub：CIS 關鍵安全控制 v8 IG3 的操作最佳實踐。

## CIS 前 20 項的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網際網路安全中心 (CIS) 前 20 大關鍵安全性控制與 AWS 受管 Config 規則之間的對應範例。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 CIS 前 20 個控制項相關。一個 CIS 前 20 項控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

本一致性套件由 AWS 安全保證服務 LLC (AWS SAS) 驗證，該公司是由支付卡產業合格安全評估機構 (QSA)、HITRUST 認證共同安全框架從業人員 (CCSFP) 以及經過認證的合規專業人員組成的團隊，可為各種產業框架提供指導和評估。 AWS SAS 專業人員設計了此一符合性包，使客戶能夠與 CIS Top 20 的子集保持一致。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.2 | ec2-檢managedinstance-association-compliance-status查 | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| CIS.2 | ec2-檢managedinstance-patch-compliance-status查 | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CIS.2 | EC2-埃security-group-attached-to尼 | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控庫存清單中未使用的安全群組並管理您的環境。 |
| CIS.2 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.2 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CIS.2 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| CIS.3 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.3 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CIS.3 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CIS.4 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CIS.4 | iam-root-access-key-檢查 | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| CIS.4 | root-account-hardware-mfa啟用 | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.4 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CIS.4 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CIS.5 | ec2-管instance-managed-by-systems理器 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.5 | ec2-檢managedinstance-association-compliance-status查 | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| CIS.5 | ec2-檢managedinstance-patch-compliance-status查 | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CIS.5 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.5 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| CIS.6 | api-gw-execution-logging啟用 | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CIS.6 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CIS.6 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.6 | cloud-trail-log-file-驗證啟用 | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CIS.6 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶 資訊、IP 地址和事件時間。 |
| CIS.6 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.6 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CIS.6 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CIS.6 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.6 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重檔案，則會將日誌檔從所有儲存貯體傳遞 AWS 區域 到 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CIS.6 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.6 | S3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CIS.6 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CIS.6 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.8 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CIS.9 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.9 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.9 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.9 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CIS.9 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.9 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.9 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為使用邏輯隔離而更加安全。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| CIS.9 | internet-gateway-authorized-vpc-只有 | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CIS.9 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.9 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| CIS.9 | rds-instance-public-access-檢查 | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CIS.9 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.9 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CIS.9 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.9 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CIS.9 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CIS.9 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.9 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| CIS.9 | vpc-default-security-group-關閉 | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CIS.9 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.10 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| CIS.10 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CIS.10 | elasticache-redis-cluster-automatic-備份檢查 | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CIS.10 | S3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.10 | S3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| CIS.11 | EC2-埃security-group-attached-to尼 | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控庫存清單中未使用的安全群組並管理您的環境。 |
| CIS.11 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.11 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CIS.11 | vpc-default-security-group-關閉 | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CIS.11 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.12 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.12 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.12 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.12 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CIS.12 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為使用邏輯隔離而更加安全。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| CIS.12 | internet-gateway-authorized-vpc-只有 | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CIS.12 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| CIS.12 | rds-instance-public-access-檢查 | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CIS.12 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CIS.12 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CIS.12 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CIS.12 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| CIS.12 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CIS.12 | vpc-default-security-group-關閉 | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.12 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CIS.13 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| CIS.13 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIS.13 | api-gw-cache-enabled和加密 | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.13 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| CIS.13 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| CIS.13 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIS.13 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CIS.13 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.13 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CIS.13 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CIS.13 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CIS.13 | kms-cmk-not-scheduled-換刪除 | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.13 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIS.13 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIS.13 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| CIS.13 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.13 | S3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| CIS.13 | bucket-server-side-encryption 啟用 S3- | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| CIS.13 | S3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIS.13 | sagemaker-endpoint-configuration-kms-密鑰配置 | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.13 | sagemaker-notebook-instance-kms-密鑰配置 | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| CIS.13 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIS.14 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| CIS.14 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | api-gw-cache-enabled和加密 | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIS.14 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| CIS.14 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| CIS.14 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.14 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.14 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIS.14 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CIS.14 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| CIS.14 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| CIS.14 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CIS.14 | kms-cmk-not-scheduled-換刪除 | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | rds-instance-public-access-檢查 | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CIS.14 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIS.14 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CIS.14 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CIS.14 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIS.14 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | S3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| CIS.14 | S3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| CIS.14 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CIS.14 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | bucket-server-side-encryption 啟用 S3- | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| CIS.14 | S3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIS.14 | sagemaker-endpoint-configuration-kms-密鑰配置 | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| CIS.14 | sagemaker-notebook-instance-kms-密鑰配置 | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.14 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIS.16 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| CIS.16 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.16 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CIS.16 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| CIS.16 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.16 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.16 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和互聯網安全中心（CIS）AWS 基準密碼強度基準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireSymbols (AWS 基礎安全最佳做法值：true)、RequireNumbers (AWS 基礎安全最佳做法值：true)、MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| CIS.16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.16 | iam-root-access-key-檢查 | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| CIS.16 | iam-user-group-membership-檢查 | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| CIS.16 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| CIS.16 | iam-user-no-policies-檢查 | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.16 | iam-user-unused-credentials-檢查 | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CIS.16 | mfa-enabled-for-iam-控制台訪問 | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| CIS.16 | root-account-hardware-mfa啟用 | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.16 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| CIS.16 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用期間，並可能降低密碼洩漏時所造成的業務影響。 |
| CIS.16 | secretsmanager-scheduled-rotation-success-檢查 | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.16 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CIS.18 | codebuild-project-envvar-awscred-檢查 | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| CIS.18 | codebuild-project-source-repo-網址檢查 | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.19 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CIS.19 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| CIS.19 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CIS.2 | ec2-管instance-managed-by-systems理器 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

### 範本

該模板可用於 GitHub：獨聯體前 20 名的操作最佳實踐。

## CISA 網路基礎的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了網絡安全與基礎設施安全局（CISA）網絡基本要點（CE）和 AWS 託管 Config 規則之間的示例映射。每個 AWS Config 規則適用於特定的 AWS 資源，並涉及到一個或多個 CISA CE 控制。CISA CE 控制項可以與多個 AWS Config 規則有關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的員工-1 | 培養意識文化，鼓勵員工在線上做出正確的選擇。 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的員工-2 | 了解網路釣魚和公司電子郵件洩露等風險。XXXXX。 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |
| 您的員工-3 | 使用學到的經驗和報告的事件，對當前的威脅環境保持警惕並靈敏因應網路安全趨勢，以便對與網路安全相關的當前事件保持認識。 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |
| 您的員工-4 | 利用基本網路安全訓練，進一步了解與實作網路安全最佳實務相關的網路安全概念、術語和活動。 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |
| 你的員工-5 | 透過專業協會、學術機構、私營機構及政府來源，找出可用的訓練資源。 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-1 | 了解您的網路上有哪些項目。維護軟硬體資產的庫存清單，以了解哪些項目正在運作以及哪些項目面臨遭受攻擊的風險。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| 您的系統-1 | 了解您的網路上有哪些項目。維護軟硬體資產的庫存清單，以了解哪些項目正在運作以及哪些項目面臨遭受攻擊的風險。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-1 | 了解您的網路上有哪些項目。維護軟硬體資產的庫存清單，以了解哪些項目正在運作以及哪些項目面臨遭受攻擊的風險。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 您的系統-1 | 了解您的網路上有哪些項目。維護軟硬體資產的庫存清單，以了解哪些項目正在運作以及哪些項目面臨遭受攻擊的風險。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-1 | 了解您的網路上有哪些項目。維護軟硬體資產的庫存清單，以了解哪些項目正在運作以及哪些項目面臨遭受攻擊的風險。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 您的系統-1 | 了解您的網路上有哪些項目。維護軟硬體資產的庫存清單，以了解哪些項目正在運作以及哪些項目面臨遭受攻擊的風險。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-1 | 了解您的網路上有哪些項目。維護軟硬體資產的庫存清單，以了解哪些項目正在運作以及哪些項目面臨遭受攻擊的風險。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| 您的系統-2 | 利用所有作業系統和第三方軟體的自動更新。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 您的系統-2 | 利用所有作業系統和第三方軟體的自動更新。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-2 | 利用所有作業系統和第三方軟體的自動更新。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 您的系統-2 | 利用所有作業系統和第三方軟體的自動更新。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的爭用，為 Amazon EBS 磁碟區提供最有效率的效能。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | opensearch-data-node-fault-tolerance | Amazon OpenSearch 服務 (服OpenSearch 務) 至少需要三個資料節點才能達到高可用性和容錯能力。部署具有至少三個資料節點的 OpenSearch Service 網域可確保節點失敗時的叢集作業。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | secretsmanager-secret-periodic-rotation | 此規則可確保「AWS Secrets Manager」密碼已啟用定期輪換。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。預設值為 90 天。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 您的系統-3 | 為所有軟硬體資產實作安全組態。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的系統-4 | 從系統中移除不支援或未經授權的軟硬體。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 您的周圍環境-1 | 了解您的網路上有哪些人員。維護網路連線的庫存清單 (使用者、供應商、業務合作夥伴等)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的周圍環境-1 | 了解您的網路上有哪些人員。維護網路連線的庫存清單 (使用者、供應商、業務合作夥伴等)。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 您的周圍環境-1 | 了解您的網路上有哪些人員。維護網路連線的庫存清單 (使用者、供應商、業務合作夥伴等)。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| 您的周圍環境-2 | 從特殊權限使用者、管理使用者和遠端存取使用者開始，對所有使用者使用多重要素驗證。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的周圍環境-2 | 從特殊權限使用者、管理使用者和遠端存取使用者開始，對所有使用者使用多重要素驗證。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 您的周圍環境-2 | 從特殊權限使用者、管理使用者和遠端存取使用者開始，對所有使用者使用多重要素驗證。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的周圍環境-2 | 從特殊權限使用者、管理使用者和遠端存取使用者開始，對所有使用者使用多重要素驗證。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 您的周圍環境-3 | 根據和最小權限授予訪問權限 need-to-know 和管理權限。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的周圍環境-3 | 根據和最小權限授予訪問權限 need-to-know 和管理權限。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 您的周圍環境-3 | 根據和最小權限授予訪問權限 need-to-know 和管理權限。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 您的周圍環境-3 | 根據和最小權限授予訪問權限 need-to-know 和管理權限。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的周圍環境-3 | 根據和最小權限授予訪問權限 need-to-know 和管理權限。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 您的周圍環境-3 | 根據和最小權限授予訪問權限 need-to-know 和管理權限。 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的周圍環境-3 | 根據和最小權限授予訪問權限 need-to-know 和管理權限。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的周圍環境-4 | 為所有使用者使用唯一密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 您的資料-1 | 了解您的資料如何受到保護。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-1 | 了解您的資料如何受到保護。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 您的資料-2 | 瞭解網路上發生的事情。管理網路和周邊元件、主機和裝置元件，以及傳輸中 data-at-rest 和使用者行為活動。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-3 | 網域名稱系統保護。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的爭用，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的資料-4 | 建立主要系統的定期自動備份和備援。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 您的資料-5 | 利用備份保護，包括實體安全、加密及離線副本。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 您的資料-5 | 利用備份保護，包括實體安全、加密及離線副本。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 您的危機回應-2 | 引導開發內部報告結構以偵測、傳達及遏制攻擊。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 您的危機回應-2 | 引導開發內部報告結構以偵測、傳達及遏制攻擊。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的爭用，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 啟動：首要執行事項-1 | 使用可自動持續備份重要資料和系統組態的備份解決方案。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-2 | 盡可能要求使用多重要素驗證 (MFA) 來存取您的系統。所有使用者都必須使用 MFA，但請從特殊權限使用者、管理使用者和遠端存取使用者開始。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| 啟動：首要執行事項-2 | 盡可能要求使用多重要素驗證 (MFA) 來存取您的系統。所有使用者都必須使用 MFA，但請從特殊權限使用者、管理使用者和遠端存取使用者開始。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-2 | 盡可能要求使用多重要素驗證 (MFA) 來存取您的系統。所有使用者都必須使用 MFA，但請從特殊權限使用者、管理使用者和遠端存取使用者開始。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 啟動：首要執行事項-2 | 盡可能要求使用多重要素驗證 (MFA) 來存取您的系統。所有使用者都必須使用 MFA，但請從特殊權限使用者、管理使用者和遠端存取使用者開始。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 啟動：首要執行事項-3 | 盡可能啟用自動更新。取代不支援的作業系統、應用程式及硬體。快速測試和部署修補程式。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-3 | 盡可能啟用自動更新。取代不支援的作業系統、應用程式及硬體。快速測試和部署修補程式。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 啟動：首要執行事項-3 | 盡可能啟用自動更新。取代不支援的作業系統、應用程式及硬體。快速測試和部署修補程式。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 啟動：首要執行事項-3 | 盡可能啟用自動更新。取代不支援的作業系統、應用程式及硬體。快速測試和部署修補程式。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

### 範本

模板是可用的 GitHub:運營最佳實踐 CISA 網絡要點.

## 刑事司法資訊服務 (CJIS) 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了刑事司法資訊服務 (CJIS) 合規要求與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 CJIS 控制項相關。一個 CJIS 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.2 | 安全意識訓練 | security-awareness-program-exists (處理程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |
| 5.3 | 事件反應 | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |
| 5.3 | 事件反應 | response-plan-tested (處理程序檢查) | 確保事件回應和復原計畫都經過測試。這有助於了解計畫在事件期間是否有效，以及是否需要因應任何差距或更新。 |
| 5.4 | 稽核與責任 | audit-log-policy-exists（過程檢查） | 建立並維護稽核日誌管理政策，以定義組織的日誌記錄要求。這包括但不限於檢閱和保留稽核日誌。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | [api-gw-execution-logging-enabled] | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 5.4.1 | 可稽核的事件與內容 (資訊系統) | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 5.4.5 | 保護稽核資訊 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.5 | 保護稽核資訊 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 5.4.5 | 保護稽核資訊 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密。 |
| 5.4.6 | 保留稽核記錄 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.4.6 | 保留稽核記錄 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| 5.5.2 | 強制存取 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 5.5.2 | 強制存取 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2 | 強制存取 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2 | 強制存取 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2 | 強制存取 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地為 IAM 密碼政策設定 RequireUppercaseCharacters RequireLowercaseCharacters (CJIS 值：假)、 RequireSymbols (CJIS 值：假)、 RequireNumbers (CJIS 值：假)、 MinimumPasswordLength (CJIS 值：8)、 PasswordReusePrevention (CJIS 值：10) 和 MaxPasswordAge (CJIS 值：90)。實際值應反映貴組織的政策。 |
| 5.5.2 | 強制存取 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2 | 強制存取 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 5.5.2 | 強制存取 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 5.5.2 | 強制存取 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2 | 強制存取 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 5.5.2 | 強制存取 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2 | 強制存取 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 5.5.2 | 強制存取 | rds-instance-iam-authentication-enabled | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體上啟用 AWS 身分和存取管理 (IAM) 身份驗證，以控制對系統和資產的存取。這會強制使用 Secure Sockets Layer (SSL) 來加密往返資料庫的網路流量。您不需要將使用者憑證放在資料庫，因為身分驗證是由外部管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2 | 強制存取 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 5.5.2.1 | 最低權限 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |
| 5.5.2.1 | 最低權限 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2.1 | 最低權限 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2.1 | 最低權限 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 5.5.2.1 | 最低權限 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2.1 | 最低權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 5.5.2.1 | 最低權限 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 5.5.2.1 | 最低權限 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2.1 | 最低權限 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 5.5.2.1 | 最低權限 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2.1 | 最低權限 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 5.5.2.1 | 最低權限 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| 5.5.2.1 | 最低權限 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.2.1 | 最低權限 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |
| 5.5.6 | 遠端存取 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.5.6 | 遠端存取 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.6.2.1.1 | 密碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地為 IAM 密碼政策設定 RequireUppercaseCharacters RequireLowercaseCharacters (CJIS 值：假)、 RequireSymbols (CJIS 值：假)、 RequireNumbers (CJIS 值：假)、 MinimumPasswordLength (CJIS 值：8)、 PasswordReusePrevention (CJIS 值：10) 和 MaxPasswordAge (CJIS 值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.6.2.2 | 進階驗證 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 5.6.2.2 | 進階驗證 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.6.2.2 | 進階驗證 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 5.6.2.2 | 進階驗證 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.6.2.2 | 進階驗證 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 5.6.3.1 | 識別符管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 5.7.1.1 | 最少功能 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 5.7.1.1 | 最少功能 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 5.7.1.1 | 最少功能 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| 5.7.1.1 | 最少功能 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 5.7.1.1 | 最少功能 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 5.7.1.1 | 最少功能 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 5.7.1.1 | 最少功能 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 5.7.1.1 | 最少功能 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 5.7.1.1 | 最少功能 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 5.7.1.1 | 最少功能 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 5.7.1.1 | 最少功能 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 5.7.1.1 | 最少功能 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 5.7.1.1 | 最少功能 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 5.7.1.1 | 最少功能 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 5.7.1.1 | 最少功能 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.7.1.1 | 最少功能 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 5.7.1.1 | 最少功能 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 5.10 | 系統與通訊保護和資訊完整性 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10 | 系統與通訊保護和資訊完整性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10 | 系統與通訊保護和資訊完整性 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10 | 系統與通訊保護和資訊完整性 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10 | 系統與通訊保護和資訊完整性 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10 | 系統與通訊保護和資訊完整性 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10 | 系統與通訊保護和資訊完整性 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 5.10 | 系統與通訊保護和資訊完整性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10 | 系統與通訊保護和資訊完整性 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 5.10 | 系統與通訊保護和資訊完整性 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10 | 系統與通訊保護和資訊完整性 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 5.10 | 系統與通訊保護和資訊完整性 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| 5.10 | 系統與通訊保護和資訊完整性 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1 | 強制執行資訊流程 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1 | 強制執行資訊流程 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1 | 強制執行資訊流程 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1 | 強制執行資訊流程 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1 | 強制執行資訊流程 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 5.10.1 | 強制執行資訊流程 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 5.10.1 | 強制執行資訊流程 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 5.10.1 | 強制執行資訊流程 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 5.10.1 | 強制執行資訊流程 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 5.10.1 | 強制執行資訊流程 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 5.10.1 | 強制執行資訊流程 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 5.10.1 | 強制執行資訊流程 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 5.10.1 | 強制執行資訊流程 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 5.10.1 | 強制執行資訊流程 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 5.10.1 | 強制執行資訊流程 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 5.10.1 | 強制執行資訊流程 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1 | 強制執行資訊流程 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 5.10.1.1 | 邊界防護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.1 | 邊界防護 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| 5.10.1.1 | 邊界防護 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 5.10.1.1 | 邊界防護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.1 | 邊界防護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 5.10.1.1 | 邊界防護 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.1 | 邊界防護 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 5.10.1.1 | 邊界防護 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 5.10.1.1 | 邊界防護 | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| 5.10.1.1 | 邊界防護 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.1 | 邊界防護 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，則 Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| 5.10.1.2 | 加密 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 5.10.1.2 | 加密 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 5.10.1.2 | 加密 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 5.10.1.2 | 加密 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密。 |
| 5.10.1.2 | 加密 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 5.10.1.2 | 加密 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 5.10.1.2 | 加密 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 5.10.1.2 | 加密 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 5.10.1.2 | 加密 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 5.10.1.2 | 加密 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 5.10.1.2 | 加密 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 5.10.1.2 | 加密 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.2 | 加密 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 5.10.1.2 | 加密 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 5.10.1.3 | 入侵偵測工具與技術 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.3 | 入侵偵測工具與技術 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.1.3 | 入侵偵測工具與技術 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.4.1 | 修補管理 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 5.10.4.1 | 修補管理 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.4.1 | 修補管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 5.10.4.1 | 修補管理 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補管理，請更新您的服務獨立任務以使用最新的平台版本。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.4.1 | 修補管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 5.10.4.4 | 安全提醒和建議 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.4.4 | 安全提醒和建議 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5.10.4.4 | 安全提醒和建議 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

### 範本

該範本位於 GitHub：CJIS 的操作最佳實踐。

## CMMC 第 1 級的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網路安全成熟度模型認證 (CMMC) 第 1 級與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CMMC 層級 1 控制項相關。一個 CMMC 第 1 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 序，或是裝置 (包括其他資訊系統)。 | | Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.211 | 在組織資訊系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

### 範本

該模板可在以下位置獲得 GitHub：CMMC 第 1 級的營運最佳實踐。

## CMMC 第 2 級的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網路安全成熟度模型認證 (CMMC) 第 2 級與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CMMC 層級 2 控制項相關。一個 CMMC 第 2 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關聯許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC.2.013 | 監視並控制遠端存取工作階段。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.2.159 | 制定並實作旨在更正缺陷並減少或消除組織系統漏洞的行動計畫。 | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.078 | 建立新密碼時，強制執行最低密碼複雜度並變更字元。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.079 | 禁止在指定的世代數目內重複使用密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於發佈的訊息中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.2.093 | 偵測和報告事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| IR.2.093 | 偵測和報告事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| RE.2.137 | 定期執行和測試資料備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| RE.2.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | vuln-scans-performed (處理程序檢查) | 確保根據您的合規需求執行漏洞掃描。貴組織應定義掃描的頻率、使用的工具以及結果的使用方式。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.1.211 | 在組織資訊系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

## 範本

該模板可在以下位置獲得 GitHub：CMMC 2 級的營運最佳實踐。

# CMMC 第 3 級的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網路安全成熟度模型認證 (CMMC) 第 3 級與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CMMC 層級 3 控制項相關。一個 CMMC 第 3 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

> **Note**
>
> 由於 DoD 和 CMMC 認證機構就 CMMC 第 3 至 5 級相互關係提供的暫定指引，因此建議客戶目前使用 AWS GovCloud （美國）區域來處理任何需要符合 CMMC 第 3 至 5 級的工作負載。因此，為了避免混淆，CMMC 第 3-5 級的一致性套件範本無法在一致性套件主控台中使用。客戶可以 CloudFormation 使用本文件中連結的範例 YAML 檔案，獨立安裝 Config 規則，以對應 CMMC 第 3-5 級的暫定性指引 (不含一致性套件範本)。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值： |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 90)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關聯許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC.2.013 | 監視並控制遠端存取工作階段。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低身分獲得或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密功能。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AU.3.051 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.051 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CA.2.159 | 制定並實作旨在更正缺陷並減少或消除組織系統漏洞的行動計畫。 | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.078 | 建立新密碼時，強制執行最低密碼複雜度並變更字元。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.079 | 禁止在指定的世代數目內重複使用密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於發佈的訊息中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.086 | 在定義的閒置期過後停用識別符。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.086 | 在定義的閒置期過後停用識別符。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsageAge 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| IR.2.093 | 偵測和報告事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| IR.2.093 | 偵測和報告事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| RE.2.137 | 定期執行和測試資料備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| RE.2.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.187 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC.3.187 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.190 | 保護通訊工作階段的真確性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.190 | 保護通訊工作階段的真確性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密功能。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.1.211 | 在組織資訊系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.213 | 定期掃描資訊系統，並在下載、開啟或執行外部來源的檔案時，即時掃描這些檔案。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

## 範本

該模板可在以下位置獲得 GitHub：CMMC 第 3 級的營運最佳實踐。

# CMMC 第 4 級的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網路安全成熟度模型認證 (CMMC) 第 4 級與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CMMC 層級 4 控制項相關。一個 CMMC 第 4 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

> **Note**
>
> 由於 DoD 和 CMMC 認證機構就 CMMC 第 3 至 5 級互惠提供的暫定指引，因此建議客戶目前使用 AWS GovCloud （美國）區域來處理任何需要符合 CMMC 第 3 至 5 級的工作負載。因此，為了避免混淆，CMMC 第 3-5 級的一致性套件範本無法在一致性套件主控台中使用。客戶可以 CloudFormation 使用本文件中連結的範例 YAML 檔案，獨立安裝 Config 規則，以對應 CMMC 第 3-5 級的暫定性指引 (不含一致性套件範本)。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值： |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 90)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關聯許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC.2.013 | 監視並控制遠端存取工作階段。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedAc tionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低身分獲得或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AM.4.226 | 運用功能來探索並識別庫存中具有特定元件屬性 (例如韌體層級、作業系統類型) 的系統。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| AM.4.226 | 運用功能來探索並識別庫存中具有特定元件屬性 (例如韌體層級、作業系統類型) 的系統。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AM.4.226 | 運用功能來探索並識別庫存中具有特定元件屬性 (例如韌體層級、作業系統類型) 的系統。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AU.3.051 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.051 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.054 | 除了每部電腦的活動之外，還可針對廣泛的活動檢閱稽核資訊。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU.4.054 | 除了每部電腦的活動之外，還可針對廣泛的活動檢閱稽核資訊。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.054 | 除了每部電腦的活動之外，還可針對廣泛的活動檢閱稽核資訊。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.078 | 建立新密碼時，強制執行最低密碼複雜度並變更字元。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.079 | 禁止在指定的世代數目內重複使用密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於發佈的訊息中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.086 | 在定義的閒置期過後停用識別符。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.086 | 在定義的閒置期過後停用識別符。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.2.093 | 偵測和報告事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| IR.2.093 | 偵測和報告事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| RE.2.137 | 定期執行和測試資料備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| RM.4.150 | 利用威脅情報提供資訊，以協助進行系統和安全架構開發、安全解決方案選擇、監控、威脅追捕，以及回應和復原活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SA.4.171 | 建立並維護網路威脅追捕功能，以搜尋組織系統中的入侵指標，並偵測、追蹤和中斷規避現有控制的威脅。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.187 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC.3.187 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.190 | 保護通訊工作階段的真確性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.190 | 保護通訊工作階段的真確性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.4.199 | 利用威脅情報以主動封鎖 DNS 請求送達惡意網域。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.4.199 | 利用威脅情報以主動封鎖 DNS 請求送達惡意網域。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SC.4.202 | 採用機制來分析可執行程式碼和指令碼 (例如沙箱)，遍歷網際網路邊界或其他組織定義的界限。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.1.211 | 在組織資訊系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.213 | 定期掃描資訊系統，並在下載、開啟或執行外部來源的檔案時，即時掃描這些檔案。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.4.221 | 利用與受保護資訊和系統相關的威脅指標資訊，以及從外部組織取得的有效緩解措施，提供資訊以進行入侵偵測和威脅追捕。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

### 範本

該模板可在以下位置獲得 GitHub：CMMC 第 4 級的操作最佳實踐。

## CMMC 第 5 級的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網路安全成熟度模型認證 (CMMC) 第 5 級與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CMMC 層級 5 控制項相關。一個 CMMC 第 5 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

> **Note**
>
> 由於 DoD 和 CMMC 認證機構就 CMMC 第 3 至 5 級互惠提供的暫定指引，因此建議客戶目前使用 AWS GovCloud （美國）區域來處理任何需要符合 CMMC 第 3 至 5 級的工作負載。因此，為了避免混淆，CMMC 第 3-5 級的一致性套件範本無法在一致性套件主控台中使用。客戶可以 CloudFormation 使用本文件中連結的範例 YAML 檔案，獨立安裝 Config 規則，以對應 CMMC 第 3-5 級的暫定性指引 (不含一致性套件範本)。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 序，或是裝置 (包括其他資訊系統)。 | | Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.001 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.1.002 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.1.003 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.007 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關聯許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.2.008 | 存取非安全功能時，請使用非特殊權限的帳戶或角色。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AC.2.013 | 監視並控制遠端存取工作階段。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC.2.013 | 監視並控制遠端存取工作階段。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.013 | 監視並控制遠端存取工作階段。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.2.016 | 根據核准的授權控制 CUI 的流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.3.014 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.017 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低身分獲得或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.3.018 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.4.023 | 控制連線系統上安全網域之間的資訊流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.5.024 | 識別並降低與連線至網路無法辨識之無線存取點相關聯的風險。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| AM.4.226 | 運用功能來探索並識別庫存中具有特定元件屬性 (例如韌體層級、作業系統類型) 的系統。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AM.4.226 | 運用功能來探索並識別庫存中具有特定元件屬性 (例如韌體層級、作業系統類型) 的系統。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| AM.4.226 | 運用功能來探索並識別庫存中具有特定元件屬性 (例如韌體層級、作業系統類型) 的系統。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.041 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.2.042 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AU.3.046 | 稽核日誌記錄程序失敗時發出提醒。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| AU.3.049 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AU.3.051 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.3.051 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.053 | 自動分析稽核日誌，以識別關鍵指標 (TTP) 和/或組織定義的可疑活動並採取行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.054 | 除了每部電腦的活動之外，還可針對廣泛的活動檢閱稽核資訊。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU.4.054 | 除了每部電腦的活動之外，還可針對廣泛的活動檢閱稽核資訊。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.4.054 | 除了每部電腦的活動之外，還可針對廣泛的活動檢閱稽核資訊。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU.5.055 | 識別未報告稽核日誌的資產，並確保適當的組織定義系統正在進行日誌記錄。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.3.161 | 持續監控安全控制，以確保控制持續有效。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| CM.2.061 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存 (包括硬體、軟體、韌體及文件)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CM.2.062 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.063 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.064 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CM.2.065 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.3.068 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CM.5.074 | 驗證組織所定義的關鍵安全性或基本軟體的完整性與正確性 (例如，信任根、正式驗證或加密簽章)。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.5.074 | 驗證組織所定義的關鍵安全性或基本軟體的完整性與正確性 (例如，信任根、正式驗證或加密簽章)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.5.074 | 驗證組織所定義的關鍵安全性或基本軟體的完整性與正確性 (例如，信任根、正式驗證或加密簽章)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.5.074 | 驗證組織所定義的關鍵安全性或基本軟體的完整性與正確性 (例如，信任根、正式驗證或加密簽章)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| IA.1.076 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.1.077 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.078 | 建立新密碼時，強制執行最低密碼複雜度並變更字元。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.079 | 禁止在指定的世代數目內重複使用密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於發佈的訊息中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| IA.2.081 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.3.083 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.086 | 在定義的閒置期過後停用識別符。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.3.086 | 在定義的閒置期過後停用識別符。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.092 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.2.093 | 偵測和報告事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.2.093 | 偵測和報告事件。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| IR.2.093 | 偵測和報告事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.5.102 | 搭配使用手動和自動程序，即時回應符合事件模式的異常活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR.5.102 | 搭配使用手動和自動程序，即時回應符合事件模式的異常活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.5.102 | 搭配使用手動和自動程序，即時回應符合事件模式的異常活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.5.102 | 搭配使用手動和自動程序，即時回應符合事件模式的異常活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| MA.2.113 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |
| RE.2.137 | 定期執行和測試資料備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| RE.2.137 | 定期執行和測試資料備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.2.137 | 定期執行和測試資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| RE.2.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| RE.3.139 | 依照組織定義定期執行完整、全面且彈性的資料備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| RE.5.140 | 確保資訊處理設施符合組織定義的資訊安全持續性、備援和可用性要求。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.2.142 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| RM.4.150 | 利用威脅情報提供資訊，以協助進行系統和安全架構開發、安全解決方案選擇、監控、威脅追捕，以及回應和復原活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| RM.4.151 | 在組織的網際網路邊界和其他組織定義的邊界上，對跨周邊網路邊界可用的未授權連接埠執行掃描。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SA.4.171 | 建立並維護網路威脅追捕功能，以搜尋組織系統中的入侵指標，並偵測、追蹤和中斷規避現有控制的威脅。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.1.175 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.2.179 | 使用加密的工作階段來管理網路裝置。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCES_ID 和 AWS_秘密 _ 碼在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SC.3.180 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.182 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.185 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.187 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC.3.187 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.190 | 保護通訊工作階段的真確性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.3.190 | 保護通訊工作階段的真確性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.190 | 保護通訊工作階段的真確性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.3.191 | 保護靜態 CUI 的機密性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.4.199 | 利用威脅情報以主動封鎖 DNS 請求送達惡意網域。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.4.199 | 利用威脅情報以主動封鎖 DNS 請求送達惡意網域。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SC.4.202 | 採用機制來分析可執行程式碼和指令碼 (例如沙箱)，遍歷網際網路邊界或其他組織定義的界限。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.198 | 設定監控系統，記錄通過組織網際網路邊界和其他組織定義邊界的封包。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC.5.198 | 設定監控系統，記錄通過組織網際網路邊界和其他組織定義邊界的封包。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.198 | 設定監控系統，記錄通過組織網際網路邊界和其他組織定義邊界的封包。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SC.5.208 | 除了市售解決方案之外，還採用組織定義和量身打造的邊界保護。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SC.5.230 | 強制執行連接埠和通訊協定合規。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.210 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.1.211 | 在組織資訊系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.1.213 | 定期掃描資訊系統，並在下載、開啟或執行外部來源的檔案時，即時掃描這些檔案。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.214 | 監控系統安全提醒和建議，並採取回應行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.216 | 監控組織系統，包括輸入和輸出通訊流量，以偵測攻擊和潛在攻擊的指標。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.2.217 | 識別未經授權使用組織系統的情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.4.221 | 利用與受保護資訊和系統相關的威脅指標資訊，以及從外部組織取得的有效緩解措施，提供資訊以進行入侵偵測和威脅追捕。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.5.222 | 分析系統行為，以偵測並緩解具有惡意動作跡象的一般系統命令和指令碼執行。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.5.223 | 持續監控個人和系統元件的異常或可疑行為。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

## 範本

該模板可在以下位置獲得 GitHub：CMMC 5 級的操作最佳實踐。

# CMMC 2.0 第 1 級的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網路安全成熟度模型認證 (CMMC) 2.0 級別 1 和 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CMMC 2.0 層級 1 控制項相關。一個 CMMC 2.0 第 1 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼的作用期間，並可能降低其洩露時所造成的業務影響。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SI.L1-3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L1-3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.L1-3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L1-3.14.2 | 在組織資訊系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.L1-3.14.5 | 定期掃描資訊系統，並在下載、開啟或執行外部來源的檔案時，即時掃描這些檔案。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存映像的完整性和安全性新增一層驗證。 |

### 範本

該模板可在以下位置獲得 GitHub：CMMC 2.0 第 1 級的操作最佳實踐。

## CMMC 2.0 第 2 級的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供網路安全成熟度模型認證 (CMMC) 2.0 級別 2 和 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 CMMC 2.0 層級 2 控制項相關。一個 CMMC 2.0 第 2 級控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 序，或是裝置 (包括其他資訊系統)。 | | Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼的作用期間，並可能降低其洩露時所造成的業務影響。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | 將資訊系統存取限制為授權使用者、代表授權使用者處理的程序，或是裝置 (包括其他資訊系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.L1-3.1.2 | 將資訊系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | 驗證並控制/限制與外部資訊系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC.L2-3.1.3 | 根據核准的授權控制 CUI 的流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Managemen t (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC.L2-3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC.L2-3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並在稽核日誌中擷取此類功能的執行情況。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.12 | 監控並控制遠端存取工作階段。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AC.L2-3.1.12 | 監控並控制遠端存取工作階段。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC.L2-3.1.12 | 監控並控制遠端存取工作階段。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.12 | 監控並控制遠端存取工作階段。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC.L2-3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.L2-3.3.1 | 在所需範圍內建立並保留系統稽核日誌和記錄，以便監控、分析、調查和報告非法或未經授權的系統活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU.L2-3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.4 | 稽核日誌記錄程序失敗時發出提醒。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU.L2-3.3.4 | 稽核日誌記錄程序失敗時發出提醒。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU.L2-3.3.4 | 稽核日誌記錄程序失敗時發出提醒。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.4 | 稽核日誌記錄程序失敗時發出提醒。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU.L2-3.3.5 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.5 | 建立稽核記錄檢閱、分析和報告程序的關聯，以進行調查並回應非法、未經授權、可疑或異常活動的跡象。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| AU.L2-3.3.8 | 保護稽核資訊和稽核日誌記錄工具，以防止未經授權的存取、修改和刪除。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CA.L2-3.12.2 | 制定並實作旨在更正缺陷並減少或消除組織系統漏洞的行動計畫。 | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.L2-3.12.3 | 持續監控安全控制，以確保控制持續有效。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CA.L2-3.12.3 | 持續監控安全控制，以確保控制持續有效。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA.L2-3.12.3 | 持續監控安全控制，以確保控制持續有效。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CM.L2-3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和清查 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和清查 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.L2-3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和清查 (包括硬體、軟體、韌體及文件)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和清查 (包括硬體、軟體、韌體及文件)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CM.L2-3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和清查 (包括硬體、軟體、韌體及文件)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | 為組織系統中採用的資訊技術產品建立並強制執行安全組態設定。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CM.L2-3.4.3 | 追蹤、檢閱、核准或否決，以及記錄組織系統的變更。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CM.L2-3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | 限制、停用或防止使用不必要的程式、功能、連接埠、通訊協定和服務。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| CM.L2-3.4.9 | 控制並監控使用者安裝的軟體。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM.L2-3.4.9 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM.L2-3.4.9 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| IA.L1-3.5.1 | 識別資訊系統使用者、代表使用者處理的程序或裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.L1-3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織資訊系統的先決條件。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA.L2-3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA.L2-3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.6 | 在定義的閒置期過後停用識別符。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.6 | 在定義的閒置期過後停用識別符。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.7 | 建立新密碼時，強制執行最低密碼複雜性和字元變更。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.8 | 在指定的產生次數之後，禁止重複使用密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| IA.L2-3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.L2-3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| IR.L2-3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| IR.L2-3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR.L2-3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| IR.L2-3.6.3 | 測試組織事件回應能力。 | response-plan-tested (處理程序檢查) | 確保事件回應和復原計畫都經過測試。這有助於了解計畫在事件期間是否有效，以及是否需要因應任何差距或更新。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| MA.L2-3.7.5 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| MA.L2-3.7.5 | 須使用多重要素驗證，才能透過外部網路連線建立非本機維護工作階段，並在完成非本機維護時終止此類連線。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RA.L2-3.11.2 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| RA.L2-3.11.2 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RA.L2-3.11.2 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RA.L2-3.11.2 | 定期掃描組織系統和應用程式中的漏洞，並在找到影響這些系統和應用程式的新漏洞時進行掃描。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | 在資訊系統的外部邊界和關鍵內部邊界監控、控制及保護組織通訊 (即組織資訊系統傳輸或接收的資訊)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | emr-master-no-public-ip | 確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SC.L2-3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | 防止未經授權和意外透過共用的系統資源傳輸資訊。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L2-3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.10 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC.L2-3.13.10 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC.L2-3.13.15 | 保護通訊工作階段的真確性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L2-3.13.15 | 保護通訊工作階段的真確性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.15 | 保護通訊工作階段的真確性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.L2-3.13.15 | 保護通訊工作階段的真確性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC.L2-3.13.15 | 保護通訊工作階段的真確性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.15 | 保護通訊工作階段的真確性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC.L2-3.13.16 | 保護靜態 CUI 的機密性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L1-3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.L1-3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L1-3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.L1-3.14.2 | 在組織資訊系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L1-3.14.5 | 定期掃描資訊系統，並在下載、開啟或執行外部來源的檔案時，即時掃描這些檔案。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.L2-3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI.L2-3.14.7 | 識別未經授權使用組織系統的情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

### 範本

該模板可在以下位置獲得 GitHub：CMMC 2.0 第 2 級的操作最佳實踐。

## 運算服務的操作最佳實務

此一致性套件包含以計算服務為基礎的 AWS Config 規則。如需詳細資訊，請參閱《任何工作負載的運算》。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：運算服務的最佳營運作方式。

## 資料復原的操作最佳實務

如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：資料彈性的營運最佳實務。

## 資料庫服務的操作最佳實務

此一致性套件包含以資料庫服務為基礎的 AWS Config 規則。如需詳細資訊，請參閱上的資料庫 AWS。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板位於 GitHub：數據庫服務的操作最佳實踐。

## 資料湖和分析服務的操作最佳實務

此一致性套件包含資料湖和分析服務的 AWS Config 規則。如需詳細資訊，請參閱上的資料湖和分析 AWS。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：資料湖和分析服務的營運最佳實務。

## DevOps 的操作最佳實務

此一致性套件包含以內部為基礎的 AWS Config 規則。 DevOps AWS如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub： DevOps.

## EC2 的操作最佳實務

此一致性套件包含以 EC2 為基礎的 AWS Config 規則。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：EC2 的營運最佳實務。

## 加密和金鑰管理的操作最佳實務

如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：加密和金鑰管理的作業最佳作法。

## ENISA 中小企業網路安全指南的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了歐盟網絡安全局（ENISA）中小企業網絡安全指南和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則都適用於特定 AWS 資源，並與一或多個適用於中小企業控制的 ENISA 網路安全指南相關。一個 ENISA 中小企業網路安全指南控制可以與多個 Config 規則相關聯。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含改編自 ENISA 中小企業網路安全指南的控制映射。ENISA 中小企業網路安全指南可在 Cybersecurity guide for SMEs - 12 steps to securing your business 取得。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：發佈網路安全政策 | 網路安全應制定明確且具體的規則 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 遭受各種安全漏洞或事件侵害。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要存取控制。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | elasticsearch-encrypted-at-rest | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elasticsearch Service (Amazon ES) 網域啟用加密功能。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | elasticsearch-node-to-node-encryption-check | 確保已 node-to-node 啟用 Amazon Elasticsearch Service 的加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1_培養良好的網路安全文化：記住資料保護 | 根據歐盟一般資料保護規則 1，所有處理或儲存歐盟/歐洲經濟區居民個人資料的中小企業，都必須確保採取適當的安全控制措施來保護該資料。這包括確保代表中小企業工作的所有第三方都採取適當的安全措施。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 2_提供適當的訓練 | 定期為所有員工提供網路安全意識訓練，確保其能夠識別並因應各種網路安全威脅。這些訓練應針對中小企業量身定制，並著重於現實生活情況。為企業內負責管理網路安全的人員提供專業的網路安全訓練，確保其具備完成工作所需的技能和能力。 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4_制定事件回應計畫 | 制定正式的事件回應計畫，該計畫包含明確的指引、角色和責任，可確保以及時、專業和適當的方式回應所有安全事件。為了快速回應安全威脅，請調查可在發生可疑活動或安全漏洞時監控並建立提醒的工具。 | response-plan-exists-maintained (程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5_安全存取系統 | 鼓勵每個人使用複雜密碼，這是一組至少由三個隨機常見單字組合而成的片語，可完美結合易記性與安全性。如果您選擇使用典型密碼：- 使用小寫和大寫字元，也可以使用數字和特殊字元，使其更長。- 避免使用 " password " 之類的簡單密碼，或 " abc " 、 " 123 " 之類的字母或數字序列。- 避免使用可在線上找到的個人資訊。不論您使用的是複雜密碼還是密碼 - 請勿在其他地方重複使用這些密碼。- 不要與同事分享。- 啟用多重要素驗證。- 使用專用的密碼管理員。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5_安全存取系統 | 鼓勵每個人使用複雜密碼，這是一組至少由三個隨機常見單字組合而成的片語，可完美結合易記性與安全性。如果您選擇使用典型密碼：- 使用小寫和大寫字元，也可以使用數字和特殊字元，使其更長。- 避免使用 " password " 之類的簡單密碼，或 " abc "、" 123 " 之類的字母或數字序列。- 避免使用可在線上找到的個人資訊。不論您使用的是複雜密碼還是密碼 - 請勿在其他地方重複使用這些密碼。- 不要與同事分享。- 啟用多重要素驗證。- 使用專用的密碼管理員。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5_安全存取系統 | 鼓勵每個人使用複雜密碼，這是一組至少由三個隨機常見單字組合而成的片語，可完美結合易記性與安全性。如果您選擇使用典型密碼：- 使用小寫和大寫字元，也可以使用數字和特殊字元，使其更長。- 避免使用 " password " 之類的簡單密碼，或 " abc "、" 123 " 之類的字母或數字序列。- 避免使用可在線上找到的個人資訊。不論您使用的是複雜密碼還是密碼 - 請勿在其他地方重複使用這些密碼。- 不要與同事分享。- 啟用多重要素驗證。- 使用專用的密碼管理員。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5_安全存取系統 | 鼓勵每個人使用複雜密碼，這是一組至少由三個隨機常見單字組合而成的片語，可完美結合易記性與安全性。如果您選擇使用典型密碼：- 使用小寫和大寫字元，也可以使用數字和特殊字元，使其更長。- 避免使用 " password " 之類的簡單密碼，或 " abc "、" 123 " 之類的字母或數字序列。- 避免使用可在線上找到的個人資訊。不論您使用的是複雜密碼還是密碼 - 請勿在其他地方重複使用這些密碼。- 不要與同事分享。- 啟用多重要素驗證。- 使用專用的密碼管理員。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5_安全存取系統 | 鼓勵每個人使用複雜密碼，這是一組至少由三個隨機常見單字組合而成的片語，可完美結合易記性與安全性。如果您選擇使用典型密碼：- 使用小寫和大寫字元，也可以使用數字和特殊字元，使其更長。- 避免使用 " password " 之類的簡單密碼，或 " abc "、" 123 " 之類的字母或數字序列。- 避免使用可在線上找到的個人資訊。不論您使用的是複雜密碼還是密碼 - 請勿在其他地方重複使用這些密碼。- 不要與同事分享。- 啟用多重要素驗證。- 使用專用的密碼管理員。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：持續修補軟體並保持最新狀態 | 理想情況下，使用集中式平台來管理修補功能。對於中小企業，強烈建議執行下列作業：- 定期更新其所有軟體。- 盡可能開啟自動更新。- 識別需要手動更新的軟體和硬體。- 考慮行動裝置與 IoT 裝置。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 6_保護裝置安全：持續修補軟體並保持最新狀態 | 理想情況下，使用集中式平台來管理修補功能。對於中小企業，強烈建議執行下列作業：- 定期更新其所有軟體。- 盡可能開啟自動更新。- 識別需要手動更新的軟體和硬體。- 考慮行動裝置與 IoT 裝置。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：持續修補軟體並保持最新狀態 | 理想情況下，使用集中式平台來管理修補功能。對於中小企業，強烈建議執行下列作業：- 定期更新其所有軟體。- 盡可能開啟自動更新。- 識別需要手動更新的軟體和硬體。- 考慮行動裝置與 IoT 裝置。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 6_保護裝置安全：持續修補軟體並保持最新狀態 | 理想情況下，使用集中式平台來管理修補功能。對於中小企業，強烈建議執行下列作業：- 定期更新其所有軟體。- 盡可能開啟自動更新。- 識別需要手動更新的軟體和硬體。- 考慮行動裝置與 IoT 裝置。 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補管理，請更新您的服務獨立任務以使用最新的平台版本。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：持續修補軟體並保持最新狀態 | 理想情況下，使用集中式平台來管理修補功能。對於中小企業，強烈建議執行下列作業：- 定期更新其所有軟體。- 盡可能開啟自動更新。- 識別需要手動更新的軟體和硬體。- 考慮行動裝置與 IoT 裝置。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保護系統的最佳實務是安裝最新的修補程式。 |
| 6_保護裝置安全：持續修補軟體並保持最新狀態 | 理想情況下，使用集中式平台來管理修補功能。對於中小企業，強烈建議執行下列作業：- 定期更新其所有軟體。- 盡可能開啟自動更新。- 識別需要手動更新的軟體和硬體。- 考慮行動裝置與 IoT 裝置。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：持續修補軟體並保持最新狀態 | 理想情況下，使用集中式平台來管理修補功能。對於中小企業，強烈建議執行下列作業：- 定期更新其所有軟體。- 盡可能開啟自動更新。- 識別需要手動更新的軟體和硬體。- 考慮行動裝置與 IoT 裝置。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | elasticsearch-encrypted-at-rest | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elasticsearch Service (Amazon ES) 網域啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | elasticsearch-node-to-node-encryption-check | 確保已 node-to-node 啟用 Amazon Elasticsearch Service 的加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6_保護裝置安全：加密 | 透過資料加密來保護資料。中小企業應確保儲存在筆記型電腦、智慧型手機及平板電腦等行動裝置上的資料均經過加密。對於透過公共網路 (例如酒店或機場網 WiFi 路) 傳輸的資料，請確保資料經過加密，無論是採用虛擬私人網路 (VPN)，或使用 SSL/TLS 通訊協定透過安全連線存取網站。請確保其本身的網站採用合適的加密技術來保護透過網際網路傳輸的用戶端資料。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | netfw-policy-rule-group-associated | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包與流量流程，並定義預設流量處理。 |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空的規則群組可能會導致非預期的行為。 |
| 7_保護網路安全：使用防火牆 | 防火牆可管理進出網路的流量，其是保護中小企業系統的重要工具。應部署防火牆來保護所有重要系統，尤其應採用防火牆來保護中小企業的網路免受網際網路影響。 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空，則 Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | [api-gw-execution-logging-enabled](#) | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon Elasticsearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7_保護網路安全：檢閱遠端存取解決方案 | 中小企業應定期檢閱所有遠端存取工具以確保其安全，特別是：- 確保所有遠端存取軟體都已修補並保持最新狀態。- 限制來自可疑地理位置或某些 IP 地址的遠端存取。- 限制員工僅能遠端存取其工作所需的系統和電腦。- 對遠端存取強制使用高強度密碼，並在可能的情況下啟用多重要素驗證。- 確保已啟用監控和提醒，以警告有可疑攻擊或不尋常的可疑活動。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9_安全備份 | 為了能復原重要的結構，您應維護備份，因為其是從勒索軟體攻擊等災難中復原的有效方法。應套用以下備份規則：- 盡可能定期並自動進行備份，- 將備份與中小企業的生產環境分開保存，- 將備份加密，特別是當備份要在不同位置之間移動時，- 測試定期從備份還原資料的能力。理想情況下，應從頭到尾定期測試完整還原。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 11_保護線上網站安全 | 中小企業必須確保以安全的方式設定及維護其線上網站，並確保所有個人資料或財務詳訊資訊 (例如信用卡資料) 均獲得充分保護。這將需要對網站執行定期安全測試以識別任何潛在的安全弱點，並定期進行檢閱以確保正確維護和更新網站。 | vuln-management-plan-exists (程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。 |

## 範本

該模板可在以下位置獲得 GitHub：ENISA 中小企業網絡安全指南的最佳操作實踐。

# Esquema Nacional de Seguridad (ENS) Low 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了西班牙國家公園德塞古里達（ENS）低框架控件和託管 Config 規則之間的示例映射。AWS 每個 Config 規則都適用於特定 AWS 資源，並與一或多個西班牙 ENS Low 控制相關。一個西班牙 ENS 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含西班牙 ENS Low 架構控制的映射，上次更新日期為 2020/10/23。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a)；b)；c) | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Anexo II 4.1.2.a)；b)；c) | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a)；b)；c) | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 4.1.2.a) ; b) ; c) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Anexo II 4.1.2.a) ; b) ; c) | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Anexo II 4.1.2.a) ; b) ; c) | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Anexo II 4.1.2.a) ; b) ; c) | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| Anexo II 4.1.2.a) ; b) ; c) | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Anexo II 4.1.2.a) ; b) ; c) | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a)；b)；c) | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| Anexo II 4.1.2.b) | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |
| Anexo II 4.1.2.b) | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| Anexo II 4.1.2.b) | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| Anexo II 4.1.2.b) | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| Anexo II 4.1.2.b) | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.1.a) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Anexo II 4.2.1.a)；b) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Anexo II 4.2.4 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| Anexo II 4.2.4 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Anexo II 4.2.4 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| Anexo II 4.2.5 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.a) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.c) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| Anexo II 4.2.6.BAJO.c) | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Anexo II 4.2.6.BAJO.c) | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| Anexo II 4.2.6.BAJO.c) | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Anexo II 4.2.6.BAJO.c) | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Anexo II 4.2.6.BAJO.c) | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| Anexo II 4.2.6.BAJO.c) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Anexo II 4.2.6.BAJO.c) | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.7.BAJO | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| Anexo II 4.2.7.BAJO | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| Anexo II 4.2.7.BAJO | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.7.BAJO | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| Anexo II 4.3.1 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| Anexo II 4.3.1 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| Anexo II 4.3.1 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| Anexo II 4.3.1 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| Anexo II 4.3.2.b) | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| Anexo II 4.3.2.b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| Anexo II 4.3.2.b) | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| Anexo II 4.3.2.b) | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| Anexo II 4.3.2.b) | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| Anexo II 4.3.2.b) | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Anexo II 4.3.2.b) | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Anexo II 4.3.2.b) | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| Anexo II 4.3.2.b) | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| Anexo II 4.3.2.b) | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| Anexo II 4.3.2.b) | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Anexo II 4.3.2.b) | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Anexo II 4.3.2.b) | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| Anexo II 4.3.2.b) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| Anexo II 4.3.2.b) | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| Anexo II 4.3.4.c) | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Anexo II 4.3.8.BAJO | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Anexo II 4.3.8.BAJO | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| Anexo II 4.3.8.BAJO | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Anexo II 4.3.8.BAJO | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Anexo II 4.3.8.BAJO | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Anexo II 4.3.8.BAJO | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Anexo II 4.3.8.BAJO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Anexo II 4.3.8.BAJO | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| Anexo II 4.3.10.b) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.10.b) | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Anexo II 4.3.10.d) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| Anexo II 4.6.1 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.6.2.BASICA | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| Anexo II 5.2.3 | security-awareness-program-exists (處理程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.3.BAJO.a) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| Anexo II 5.6.1.c) | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.6.1.c) | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| Anexo II 5.7.3 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Anexo II 5.7.3 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 5.7.3 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Anexo II 5.7.3 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| Anexo II 5.7.3 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Anexo II 5.7.3 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.7.3 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Anexo II 5.7.3 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.4 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| Anexo II 5.7.4 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.2 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| Anexo II 5.8.2 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| Art. 14.4 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Art. 16 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 16 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Art. 16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Art. 16 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| Art. 20.2 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 20.2 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| Art. 20.2 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| Art. 20.2 | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |
| Art. 21.1 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| Art. 21.1 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| Art. 21.1 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| Art. 21.1 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| Art. 21.1 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發佈訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Art. 21.1 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| Art. 21.1 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Art. 21.1 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Art. 21.1 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| Art. 21.1 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Art. 21.1 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Art. 21.1 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Art. 21.1 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| Art. 21.1 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| Art. 21.1 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Art. 21.1 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| Art. 22 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| Art. 22 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| Art. 22 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| Art. 22 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| Art. 22 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Art. 22 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Art. 22 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Art. 22 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| Art. 22 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| Art. 22 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Art. 22 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Art. 22 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| Art. 22 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| Art. 22 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Art. 23 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Art. 23 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| Art. 23 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Art. 23 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Art. 23 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Art. 23 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Art. 23 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Art. 23 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| Art. 25 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| Art. 25 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| Art. 25 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| Art. 25 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| Art. 25 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| Art. 25 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

## 範本

該模板是可用的 GitHub:操作最佳實踐國家安古里達 (ENS) 低.

# Esquema Nacional de Seguridad (ENS) Medium 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了西班牙國家公園德塞古里達（ENS）中型框架控制項和託管 Config 規則之間的示例映射。AWS 每個 Config 規則適用於特定 AWS 資源，並與一個或多個西班牙 ENS Medium 控制項相關。一個西班牙 ENS 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含西班牙 ENS Medium 架構控制的映射，上次更新日期為 2020/10/23。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a)；b)；c) | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Anexo II 4.1.2.a)；b)；c) | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a)；b)；c) | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 4.1.2.a) ; b) ; c) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Anexo II 4.1.2.a) ; b) ; c) | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Anexo II 4.1.2.a) ; b) ; c) | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Anexo II 4.1.2.a) ; b) ; c) | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| Anexo II 4.1.2.a) ; b) ; c) | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Anexo II 4.1.2.a) ; b) ; c) | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a)；b)；c) | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| Anexo II 4.1.2.b) | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |
| Anexo II 4.1.2.b) | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| Anexo II 4.1.2.b) | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| Anexo II 4.1.2.b) | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| Anexo II 4.1.2.b) | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.1.a) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Anexo II 4.2.1.a)；4.2.1.b) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Anexo II 4.2.4 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| Anexo II 4.2.4 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Anexo II 4.2.4 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| Anexo II 4.2.5 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.5.a) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.5.c) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| Anexo II 4.2.6.BAJO.c) | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.c) | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Anexo II 4.2.6.c) | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Anexo II 4.2.6.c) | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.c) | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| Anexo II 4.2.6.c) | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Anexo II 4.2.6.c) | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Anexo II 4.2.6.c) | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.c) | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Anexo II 4.2.6.c) | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Anexo II 4.2.6.c) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.c) | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| Anexo II 4.2.7 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| Anexo II 4.2.7 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| Anexo II 4.2.7 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.7 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| Anexo II 4.3.1 | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |
| Anexo II 4.3.1 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| Anexo II 4.3.1 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| Anexo II 4.3.1 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| Anexo II 4.3.1 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| Anexo II 4.3.2.b) | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| Anexo II 4.3.2.b) | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| Anexo II 4.3.2.b) | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| Anexo II 4.3.2.b) | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Anexo II 4.3.2.b) | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| Anexo II 4.3.2.b) | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| Anexo II 4.3.2.b) | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Anexo II 4.3.2.b) | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Anexo II 4.3.2.b) | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| Anexo II 4.3.2.b) | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| Anexo II 4.3.2.b) | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| Anexo II 4.3.2.b) | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Anexo II 4.3.2.b) | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Anexo II 4.3.2.b) | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| Anexo II 4.3.2.b) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| Anexo II 4.3.2.b) | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| Anexo II 4.3.4.c) | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.6 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| Anexo II 4.3.7.a) | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |
| Anexo II 4.3.8 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Anexo II 4.3.8 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| Anexo II 4.3.8 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Anexo II 4.3.8 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Anexo II 4.3.8 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| Anexo II 4.3.8 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Anexo II 4.3.8 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Anexo II 4.3.8 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| Anexo II 4.3.8.BAJO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| Anexo II 4.3.10.b) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| Anexo II 4.3.10.b) | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Anexo II 4.3.10.d) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.6.1 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| Anexo II 4.6.2 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| Anexo II 4.6.2 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| Anexo II 5.2.3 | security-awareness-program-exists (處理程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.2 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.4.2 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.2 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 5.4.2 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.4.2 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2.MEDIO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.3 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.3 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.4.3 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.3 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.3 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 5.4.3 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.4.3 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.3 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.3.MEDIO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.3.a) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| Anexo II 5.6.1.c) | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.6.1.c) | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| Anexo II 5.7.3 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Anexo II 5.7.3 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 5.7.3 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Anexo II 5.7.3 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| Anexo II 5.7.3 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Anexo II 5.7.3 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.7.3 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Anexo II 5.7.3 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.4 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| Anexo II 5.7.4 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.2 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| Anexo II 5.8.2 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| Anexo II 5.8.3.b) | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.3.b) | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| Anexo II 5.8.3.b) | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| Anexo II 5.8.3.b) | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.3.b) | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Anexo II 5.8.3.b) | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| Anexo II 5.8.3.b) | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.3.b) | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| Art. 14.4 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Art. 16 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| Art. 16 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Art. 16 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| Art. 20.2 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 20.2 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| Art. 20.2 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| Art. 20.2 | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |
| Art. 21.1 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| Art. 21.1 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| Art. 21.1 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| Art. 21.1 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| Art. 21.1 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發佈訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Art. 21.1 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| Art. 21.1 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Art. 21.1 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Art. 21.1 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| Art. 21.1 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Art. 21.1 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Art. 21.1 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Art. 21.1 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| Art. 21.1 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| Art. 21.1 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Art. 21.1 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| Art. 22 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| Art. 22 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| Art. 22 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Art. 22 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| Art. 22 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| Art. 22 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| Art. 22 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Art. 22 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Art. 22 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| Art. 22 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| Art. 22 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| Art. 22 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Art. 22 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| Art. 22 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| Art. 22 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| Art. 23 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Art. 23 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| Art. 23 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| Art. 23 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Art. 23 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| Art. 23 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Art. 23 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Art. 23 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Art. 23 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| Art. 24.1 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| Art. 24.2 | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| Art. 25 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| Art. 25 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| Art. 25 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| Art. 25 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

### 範本

該模板是可用的 GitHub:操作最佳實踐國家安古里達 (ENS) 媒介.

## Esquema Nacional de Seguridad (ENS) High 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了西班牙國家公園德塞古里達（ENS）高框架控件和託管 Config 規則之間的示例映射。AWS 每個 Config 規則適用於特定 AWS 資源，並與一個或多個西班牙 ENS 高控制項相關。一個西班牙 ENS 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含西班牙 ENS High 架構控制的映射，上次更新日期為 2021/07/09。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.1.ALTO | annual-risk-assessment-performed（過程檢查） | 對貴組織執行年度風險評估。風險評估可協助判定已識別風險和/或漏洞影響組織的可能性及影響。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.2.1.b) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 4.2.5.ALTO.a) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Anexo II 4.1.2.a)；b)；c) | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Anexo II 4.1.2.a)；b)；c) | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 4.1.2.a) ; b) ; c) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Anexo II 4.1.2.a) ; b) ; c) | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Anexo II 4.1.2.a) ; b) ; c) | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Anexo II 4.1.2.a) ; b) ; c) | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 4.1.2.a) ; b) ; c) | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| Anexo II 4.1.2.a) ; b) ; c) | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Anexo II 4.1.2.a) ; b) ; c) | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| Anexo II 4.1.2.a) ; b) ; c) | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a) ; b) ; c) | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 4.1.2.a) ; b) ; c) | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.a)；b)；c) | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| Anexo II 4.1.2.b) | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |
| Anexo II 4.1.2.b) | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| Anexo II 4.1.2.b) | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| Anexo II 4.1.2.b) | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| Anexo II 4.1.2.b) | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.1.a) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Anexo II 4.2.4 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| Anexo II 4.2.4 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Anexo II 4.2.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.4 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| Anexo II 4.2.5 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.a) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.c) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| Anexo II 4.2.6.ALTO.b) | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.ALTO.b) | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| Anexo II 4.2.6.ALTO.b) | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| Anexo II 4.2.6.ALTO.b) | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Anexo II 4.2.6.BAJO.c) | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Anexo II 4.2.6.BAJO.c) | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| Anexo II 4.2.6.BAJO.c) | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Anexo II 4.2.6.BAJO.c) | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Anexo II 4.2.6.BAJO.c) | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Anexo II 4.2.6.BAJO.c) | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Anexo II 4.2.6.BAJO.c) | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| Anexo II 4.2.7.BAJO | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.2.7.BAJO | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| Anexo II 4.2.7.BAJO | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| Anexo II 4.2.7.BAJO | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| Anexo II 4.3.1 | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| Anexo II 4.3.1 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| Anexo II 4.3.1 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.1 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| Anexo II 4.3.1 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| Anexo II 4.3.2.b) | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| Anexo II 4.3.2.b) | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| Anexo II 4.3.2.b) | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| Anexo II 4.3.2.b) | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| Anexo II 4.3.2.b) | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Anexo II 4.3.2.b) | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| Anexo II 4.3.2.b) | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端中資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| Anexo II 4.3.2.b) | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| Anexo II 4.3.2.b) | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Anexo II 4.3.2.b) | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| Anexo II 4.3.2.b) | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| Anexo II 4.3.2.b) | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| Anexo II 4.3.2.b) | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Anexo II 4.3.2.b) | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Anexo II 4.3.2.b) | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.2.b) | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| Anexo II 4.3.2.b) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| Anexo II 4.3.2.b) | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| Anexo II 4.3.4.c) | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.6 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| Anexo II 4.3.7.MEDIA.a) | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |
| Anexo II 4.3.8.BAJO | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Anexo II 4.3.8.BAJO | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| Anexo II 4.3.8.BAJO | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Anexo II 4.3.8.BAJO | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Anexo II 4.3.8.BAJO | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| Anexo II 4.3.8.BAJO | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Anexo II 4.3.8.BAJO | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| Anexo II 4.3.8.BAJO | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Anexo II 4.3.8.BAJO | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Anexo II 4.3.8.MEDIO | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Anexo II 4.3.8.MEDIO | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| Anexo II 4.3.8.MEDIO | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Anexo II 4.3.8.MEDIO | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Anexo II 4.3.8.MEDIO | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Anexo II 4.3.8.MEDIO | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Anexo II 4.3.8.MEDIO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Anexo II 4.3.8.MEDIO | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| Anexo II 4.3.10.b) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.3.10.b) | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Anexo II 4.3.10.d) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| Anexo II 4.6.1 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 4.6.2.ALTO | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| Anexo II 4.6.2.BASICA | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| Anexo II 4.6.2.MEDIA | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.2.3 | security-awareness-program-exists (處理程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |
| Anexo II 5.2.4 | security-awareness-program-exists (處理程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |
| Anexo II 5.2.5 | security-awareness-program-exists (處理程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |
| Anexo II 5.4.2.MEDIO | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2.MEDIO | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.2.MEDIO | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2.MEDIO | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2.MEDIO | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 5.4.2.MEDIO | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.4.2.MEDIO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.2.MEDIO | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.2.MEDIO | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.3.BAJO.a) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| Anexo II 5.4.3.MEDIO | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.3.MEDIO | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.4.3.MEDIO | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.3.MEDIO | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.3.MEDIO | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.4.3.MEDIO | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Anexo II 5.4.3.MEDIO | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| Anexo II 5.4.3.MEDIO | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.4.3.MEDIO | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.6.1.c) | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| Anexo II 5.6.1.c) | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| Anexo II 5.7.3 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Anexo II 5.7.3 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | rds-snapshot-encrypted | 確保已針對 Amazon Relationa l Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| Anexo II 5.7.3 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Anexo II 5.7.3 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| Anexo II 5.7.3 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Anexo II 5.7.3 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| Anexo II 5.7.3 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Anexo II 5.7.3 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Anexo II 5.7.3 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| Anexo II 5.7.3 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Anexo II 5.7.3 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.3 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Anexo II 5.7.3 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.3 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Anexo II 5.7.4 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.7.4 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| Anexo II 5.8.2 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| Anexo II 5.8.2 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| Anexo II 5.8.3.MEDIO.b) | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| Anexo II 5.8.3.MEDIO.b) | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| Anexo II 5.8.3.MEDIO.b) | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Anexo II 5.8.3.MEDIO.b) | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| Anexo II 5.8.3.MEDIO.b) | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 14.4 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Art. 16 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| Art. 16 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Art. 16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 16 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| Art. 20.2 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| Art. 20.2 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| Art. 20.2 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 20.2 | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |
| Art. 21.1 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Art. 21.1 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| Art. 21.1 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| Art. 21.1 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| Art. 21.1 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| Art. 21.1 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發佈訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Art. 21.1 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| Art. 21.1 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Art. 21.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| Art. 21.1 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| Art. 21.1 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Art. 21.1 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| Art. 21.1 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| Art. 21.1 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| Art. 21.1 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Art. 21.1 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Art. 21.1 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Art. 21.1 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 21.1 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| Art. 22 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| Art. 22 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| Art. 22 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| Art. 22 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Art. 22 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| Art. 22 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端中資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| Art. 22 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| Art. 22 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Art. 22 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Art. 22 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| Art. 22 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| Art. 22 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Art. 22 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| Art. 22 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| Art. 22 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 22 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| Art. 23 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Art. 23 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| Art. 23 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| Art. 23 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Art. 23 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| Art. 23 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| Art. 23 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Art. 23 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 23 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Art. 23 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| Art. 24.2 | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 24.1 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| Art. 25 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| Art. 25 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| Art. 25 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| Art. 25 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| Art. 25 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Art. 25 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| Art. 25 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

### 範本

該模板是可用的 GitHub:操作最佳實踐國家安古里達 (ENS) 高.

## FDA 標題 21 CFR 操作最佳實務第 11 部分

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供聯邦法規 (CFR) 第 11 部分標題 21 與 AWS 受管組 Config 規則之間的範例對應。每個 AWS Config 規則都適用於特定 AWS 資源，並與一個或多個 FDA 標題 21 CFR 第 11 部分控制項相關。一個 FDA CFR 第 21 編第 11 部分控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 實。這些程序和控制措施應包括： | | |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 11.1 | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括： | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays （Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 11.10(a) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(a) 驗證系統，以確保系統正確、可靠、具有一致的預期效能，並能夠辨別無效或已更改的記錄。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | ecr-private-lifecycle-policy-configured | Amazon Elastic Container Repository (ECR) 生命週期政策可讓您指定儲存庫中映像的生命週期管理。此動作可允許自動清除未使用映像，例如根據存在時間或計數來判斷的過期映像。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 11.10(c) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(c) 保護記錄，以確保這些記錄在整個記錄保留期內正確且可供擷取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Ama zon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 11.10(d) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(d) 限制獲授權個人對系統的存取權。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | [api-gw-execution-logging-enabled](#) | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(e) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(e) 使用安全、由電腦產生且具有時間戳記的稽核記錄，獨立記錄操作員輸入和動作 (建立、修改或刪除電子記錄) 的日期和時間。記錄變更不應遮蔽先前記錄的資訊。此類稽核記錄文件應依照主體電子記錄所需至少保留一段時間，並可供機構審查和複製。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(g) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(g) 使用授權檢查，以確保只有獲授權個人才能使用系統、以電子方式簽署記錄、存取操作或電腦系統輸入或輸出裝置、更改記錄，或是執行手邊的操作。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(h) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和管制應包括以下內容：（h）使用設備（例如終端）檢查，以確定數據輸入或操作指令的來源的有效性（如終端）。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 11.10(h) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和管制應包括以下內容：（h）使用設備（例如終端）檢查，以確定數據輸入或操作指令的來源的有效性（如終端）。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(h) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和管制應包括以下內容：（h）使用設備（例如終端）檢查，以確定數據輸入或操作指令的來源的有效性（如終端）。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 11.10(i) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(i) 確定開發、維護或使用電子記錄/電子簽章系統的人員受過教育、訓練並具有經驗，能夠執行獲指派的任務。 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計畫可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.10(k) | 使用封閉系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄的真確性、完整性以及 (如果適用) 機密性，並確保簽署者無法輕易否認已簽署記錄並非真實。這些程序和控制措施應包括：(k) 對系統文件採用適當的控制，包括：(1) 對系統操作和維護文件的分發、存取和使用有足夠的控制。(2) 修訂和變更控制程序，以維護按時間順序記錄系統文件制定和修改的稽核記錄。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | (a) 未採用生物特徵辨識的電子簽章應：(1) 使用至少兩個不同的識別元件，例如識別碼和密碼。(i) 當個人在存取受控系統的一段連續時間內執行一系列簽署時，首次簽署應使用所有電子簽章元件執行；後續簽署則應使用至少一個電子簽章元件執行，而且此元件只能由該個人執行並專為僅供該個人使用所設計。(ii) 當個人在存取受控系統的一段連續時間內執行一或多次簽署時，每次簽署均應使用所有電子簽章元件執行。(2) 僅限真正的擁有者才能使用；以及 (3) 受到管理和執行，以確保除真正的擁有者以外的任何人在嘗試使用個人的電子簽章時，需要兩人或更多人的協作。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | (a) 未採用生物特徵辨識的電子簽章應：(1) 使用至少兩個不同的識別元件，例如識別碼和密碼。(i) 當個人在存取受控系統的一段連續時間內執行一系列簽署時，首次簽署應使用所有電子簽章元件執行；後續簽署則應使用至少一個電子簽章元件執行，而且此元件只能由該個人執行並專為僅供該個人使用所設計。(ii) 當個人在存取受控系統的一段連續時間內執行一或多次簽署時，每次簽署均應使用所有電子簽章元件執行。(2) 僅限真正的擁有者才能使用；以及 (3) 受到管理和執行，以確保除真正的擁有者以外的任何人在嘗試使用個人的電子簽章時，需要兩人或更多人的協作。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | (a) 未採用生物特徵辨識的電子簽章應：(1) 使用至少兩個不同的識別元件，例如識別碼和密碼。(i) 當個人在存取受控系統的一段連續時間內執行一系列簽署時，首次簽署應使用所有電子簽章元件執行；後續簽署則應使用至少一個電子簽章元件執行，而且此元件只能由該個人執行並專為僅供該個人使用所設計。(ii) 當個人在存取受控系統的一段連續時間內執行一或多次簽署時，每次簽署均應使用所有電子簽章元件執行。(2) 僅限真正的擁有者才能使用；以及 (3) 受到管理和執行，以確保除真正的擁有者以外的任何人在嘗試使用個人的電子簽章時，需要兩人或更多人的協作。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | (a) 未採用生物特徵辨識的電子簽章應：(1) 使用至少兩個不同的識別元件，例如識別碼和密碼。(i) 當個人在存取受控系統的一段連續時間內執行一系列簽署時，首次簽署應使用所有電子簽章元件執行；後續簽署則應使用至少一個電子簽章元件執行，而且此元件只能由該個人執行並專為僅供該個人使用所設計。(ii) 當個人在存取受控系統的一段連續時間內執行一或多次簽署時，每次簽署均應使用所有電子簽章元件執行。(2) 僅限真正的擁有者才能使用；以及 (3) 受到管理和執行，以確保除真正的擁有者以外的任何人在嘗試使用個人的電子簽章時，需要兩人或更多人的協作。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | (a) 未採用生物特徵辨識的電子簽章應：(1) 使用至少兩個不同的識別元件，例如識別碼和密碼。(i) 當個人在存取受控系統的一段連續時間內執行一系列簽署時，首次簽署應使用所有電子簽章元件執行；後續簽署則應使用至少一個電子簽章元件執行，而且此元件只能由該個人執行並專為僅供該個人使用所設計。(ii) 當個人在存取受控系統的一段連續時間內執行一或多次簽署時，每次簽署均應使用所有電子簽章元件執行。(2) 僅限真正的擁有者才能使用；以及 (3) 受到管理和執行，以確保除真正的擁有者以外的任何人在嘗試使用個人的電子簽章時，需要兩人或更多人的協作。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | (a) 未採用生物特徵辨識的電子簽章應：(1) 使用至少兩個不同的識別元件，例如識別碼和密碼。(i) 當個人在存取受控系統的一段連續時間內執行一系列簽署時，首次簽署應使用所有電子簽章元件執行；後續簽署則應使用至少一個電子簽章元件執行，而且此元件只能由該個人執行並專為僅供該個人使用所設計。(ii) 當個人在存取受控系統的一段連續時間內執行一或多次簽署時，每次簽署均應使用所有電子簽章元件執行。(2) 僅限真正的擁有者才能使用；以及 (3) 受到管理和執行，以確保除真正的擁有者以外的任何人在嘗試使用個人的電子簽章時，需要兩人或更多人的協作。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.2 | (a) 未採用生物特徵辨識的電子簽章應：(1) 使用至少兩個不同的識別元件，例如識別碼和密碼。(i) 當個人在存取受控系統的一段連續時間內執行一系列簽署時，首次簽署應使用所有電子簽章元件執行；後續簽署則應使用至少一個電子簽章元件執行，而且此元件只能由該個人執行並專為僅供該個人使用所設計。(ii) 當個人在存取受控系統的一段連續時間內執行一或多次簽署時，每次簽署均應使用所有電子簽章元件執行。(2) 僅限真正的擁有者才能使用；以及 (3) 受到管理和執行，以確保除真正的擁有者以外的任何人在嘗試使用個人的電子簽章時，需要兩人或更多人的協作。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.3 | 使用開放系統建立、修改、維護或傳送電子記錄的人員，應採用程序和控制措施來確保電子記錄從建立到接收的真確性、完整性以及 (如果適用) 機密性。這些程序和控制措施應包括 11.10 中所述的適當程序和控制措施，以及其他措施 (例如文件加密和使用適當的數位簽章標準)，以確保在必要情況下記錄真確性、完整性和機密性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.300(b) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。此類控制項應包括：(b) 確保定期檢查、召回或修訂識別碼和密碼問題 (例如，涵蓋密碼過時等事件)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.300(b) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。此類控制項應包括：(b) 確保定期檢查、召回或修訂識別碼和密碼問題 (例如，涵蓋密碼過時等事件)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.300(b) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。此類控制項應包括：(b) 確保定期檢查、召回或修訂識別碼和密碼問題 (例如，涵蓋密碼過時等事件)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.300(b) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。此類控制項應包括：(b) 確保定期檢查、召回或修訂識別碼和密碼問題 (例如，涵蓋密碼過時等事件)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsageAge（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 11.300(b) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。此類控制項應包括：(b) 確保定期檢查、召回或修訂識別碼和密碼問題 (例如，涵蓋密碼過時等事件)。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.300(b) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。此類控制項應包括：(b) 確保定期檢查、召回或修訂識別碼和密碼問題 (例如，涵蓋密碼過時等事件)。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 11.300(d) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。這些控制措施應包括：(d) 使用交易保護措施來防止未經授權使用密碼和/或識別碼，並立即盡快偵測和報告任何未經授權使用系統安全裝置的嘗試，然後在適當情況下向組織管理階層呈報。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.300(d) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。這些控制措施應包括：(d) 使用交易保護措施來防止未經授權使用密碼和/或識別碼，並立即盡快偵測和報告任何未經授權使用系統安全裝置的嘗試，然後在適當情況下向組織管理階層呈報。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 11.300(d) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。這些控制措施應包括：(d) 使用交易保護措施來防止未經授權使用密碼和/或識別碼，並立即盡快偵測和報告任何未經授權使用系統安全裝置的嘗試，然後在適當情況下向組織管理階層呈報。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.300(d) | 使用識別碼搭配密碼之電子簽章的人員，應採用控制措施來確保其安全和完整性。這些控制措施應包括：(d) 使用交易保護措施來防止未經授權使用密碼和/或識別碼，並立即盡快偵測和報告任何未經授權使用系統安全裝置的嘗試，然後在適當情況下向組織管理階層呈報。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

### 範本

該模板可用於 GitHub：FDA 標題 21 CFR 部分 11 的操作最佳實踐。

## FedRAMP (低) 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供聯邦風險與授權管理計畫 (FedRAMP) 低基準控制與 AWS 受管 Config 規則之間的範例對映。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 FedRAMP 控制項相關。一個 FedRAMP 控制項可以與多項 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| AC-2 | 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| AC-2 | 帳戶管理 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| AC-2 | 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-2 | 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC-2 | 帳戶管理 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2 | 帳戶管理 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC-2 | 帳戶管理 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC-2 | 帳戶管理 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AC-2 | 帳戶管理 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2 | 帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2 | 帳戶管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| AC-2 | 帳戶管理 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-2 | 帳戶管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| AC-2 | 帳戶管理 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-2 | 帳戶管理 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC-3 | 強制存取 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |
| AC-3 | 強制存取 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-3 | 強制存取 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-3 | 強制存取 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC-3 | 強制存取 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3 | 強制存取 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3 | 強制存取 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-3 | 強制存取 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| AC-3 | 強制存取 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-3 | 強制存取 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3 | 強制存取 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-3 | 強制存取 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-3 | 強制存取 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-3 | 強制存取 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-3 | 強制存取 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3 | 強制存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3 | 強制存取 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-17 | 遠端存取 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17 | 遠端存取 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-17 | 遠端存取 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17 | 遠端存取 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-17 | 遠端存取 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-17 | 遠端存取 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-17 | 遠端存取 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-17 | 遠端存取 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC-17 | 遠端存取 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-17 | 遠端存取 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-17 | 遠端存取 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-17 | 遠端存取 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-17 | 遠端存取 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-17 | 遠端存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-17 | 遠端存取 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC-17 | 遠端存取 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-17 | 遠端存取 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17 | 遠端存取 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AU-2 | 稽核事件 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-2 | 稽核事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU-2 | 稽核事件 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-2 | 稽核事件 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-2 | 稽核事件 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-2 | 稽核事件 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-2 | 稽核事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-2 | 稽核事件 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU-2 | 稽核事件 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-2 | 稽核事件 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-2 | 稽核事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-2 | 稽核事件 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄的內容 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| AU-3 | 稽核記錄的內容 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄的內容 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU-3 | 稽核記錄的內容 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-3 | 稽核記錄的內容 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄的內容 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-3 | 稽核記錄的內容 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-3 | 稽核記錄的內容 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄的內容 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-3 | 稽核記錄的內容 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄的內容 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-3 | 稽核記錄的內容 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| AU-6 | 稽核檢閱、分析及報告 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU-6 | 稽核檢閱、分析及報告 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-6 | 稽核檢閱、分析及報告 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-6 | 稽核檢閱、分析及報告 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU-6 | 稽核檢閱、分析及報告 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-6 | 稽核檢閱、分析及報告 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AU-6 | 稽核檢閱、分析及報告 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-6 | 稽核檢閱、分析及報告 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-6 | 稽核檢閱、分析及報告 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-9 | 保護稽核資訊 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| AU-9 | 保護稽核資訊 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| AU-9 | 保護稽核資訊 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-9 | 保護稽核資訊 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密功能。 |
| AU-9 | 保護稽核資訊 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| AU-11 | 保留稽核記錄 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌可提供有關組建專案的詳細資訊。 |
| AU-12 | 產生稽核 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU-12 | 產生稽核 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-12 | 產生稽核 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-12 | 產生稽核 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-12 | 產生稽核 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-12 | 產生稽核 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-12 | 產生稽核 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| CA-7 | 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| CA-7 | 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| CA-7 | 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CA-7 | 持續監控 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳號 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CA-7 | 持續監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CA-7 | 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| CM-2 | 基準組態 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| CM-2 | 基準組態 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM-2 | 基準組態 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM-2 | 基準組態 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CM-2 | 基準組態 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM-2 | 基準組態 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CM-2 | 基準組態 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM-2 | 基準組態 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM-2 | 基準組態 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM-2 | 基準組態 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM-2 | 基準組態 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM-2 | 基準組態 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CM-2 | 基準組態 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-2 | 基準組態 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| CM-2 | 基準組態 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CM-2 | 基準組態 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CM-2 | 基準組態 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可防止儲存貯體層級的公開存取，協助保護敏感資料的安全，免受未經授權的遠端使用者存取。 |
| CM-2 | 基準組態 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM-7 | 最少功能 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-7 | 最少功能 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-7 | 最少功能 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-8 | 資訊系統元件庫存清單 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-8 | 資訊系統元件庫存清單 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CM-8 | 資訊系統元件庫存清單 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM-8 | 資訊系統元件庫存清單 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CP-9 | 資訊系統備份 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9 | 資訊系統備份 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9 | 資訊系統備份 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9 | 資訊系統備份 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9 | 資訊系統備份 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9 | 資訊系統備份 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9 | 資訊系統備份 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9 | 資訊系統備份 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9 | 資訊系統備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CP-9 | 資訊系統備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-9 | 資訊系統備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9 | 資訊系統備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CP-9 | 資訊系統備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9 | 資訊系統備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| CP-10 | 資訊系統復原與重建 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 資訊系統復原與重建 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 資訊系統復原與重建 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| CP-10 | 資訊系統復原與重建 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 資訊系統復原與重建 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-10 | 資訊系統復原與重建 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| CP-10 | 資訊系統復原與重建 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CP-10 | 資訊系統復原與重建 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CP-10 | 資訊系統復原與重建 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| CP-10 | 資訊系統復原與重建 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-10 | 資訊系統復原與重建 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA-2 | 識別與驗證 (組織使用者) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA-2 | 識別與驗證 (組織使用者) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| IA-2 | 識別與驗證 (組織使用者) | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA-2 | 識別與驗證 (組織使用者) | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA-2 | 識別與驗證 (組織使用者) | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA-2 | 識別與驗證 (組織使用者) | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-5 | 驗證器管理 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA-5 | 驗證器管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-4 | 事件處理 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| IR-4 | 事件處理 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-4 | 事件處理 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-4 | 事件處理 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-4 | 事件處理 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR-6 | 事件報告 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-6 | 事件報告 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-6 | 事件報告 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| IR-7 | 事件回應協助 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-7 | 事件回應協助 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IR-7 | 事件回應協助 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RA-5 | 漏洞掃描 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RA-5 | 漏洞掃描 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| RA-5 | 漏洞掃描 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SA-3 | 系統開發生命週期 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SA-3 | 系統開發生命週期 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SA-3 | 系統開發生命週期 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SC-5 | 拒絕服務保護 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-5 | 拒絕服務保護 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| SC-5 | 拒絕服務保護 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-5 | 拒絕服務保護 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| SC-5 | 拒絕服務保護 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| SC-5 | 拒絕服務保護 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的爭用，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-5 | 拒絕服務保護 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| SC-5 | 拒絕服務保護 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| SC-5 | 拒絕服務保護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-5 | 拒絕服務保護 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-5 | 拒絕服務保護 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| SC-5 | 拒絕服務保護 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-5 | 拒絕服務保護 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SC-7 | 邊界保護 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC-7 | 邊界保護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| SC-7 | 邊界保護 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| SC-7 | 邊界保護 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-7 | 邊界保護 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC-7 | 邊界保護 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7 | 邊界保護 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7 | 邊界保護 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| SC-7 | 邊界保護 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7 | 邊界保護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-7 | 邊界保護 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7 | 邊界保護 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7 | 邊界保護 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7 | 邊界保護 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| SC-12 | 密碼編譯金鑰建立與管理 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-12 | 密碼編譯金鑰建立與管理 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| SC-12 | 密碼編譯金鑰建立與管理 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC-13 | 密碼編譯保護 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯保護 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯保護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯保護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯保護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯保護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-2 | 瑕疵修復 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SI-2 | 瑕疵修復 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-2 | 瑕疵修復 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SI-2 | 瑕疵修復 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統的最佳實務。 |
| SI-3 | 瑕疵修復 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-3 | 瑕疵修復 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| SI-3 | 瑕疵修復 | ecs-task-definition-memory-hard-limit | 限制 Amazon Elastic Container Service (ECS) 容器的可用記憶體上限，可確保當容器遇到惡意存取時，資源用量不會遭到濫用。 |
| SI-4 | 資訊系統監控 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4 | 資訊系統監控 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SI-4 | 資訊系統監控 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4 | 資訊系統監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4 | 資訊系統監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI-4 | 資訊系統監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4 | 資訊系統監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI-4 | 資訊系統監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI-4 | 資訊系統監控 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4 | 資訊系統監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4 | 資訊系統監控 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4 | 資訊系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI-4 | 資訊系統監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-5 | 安全提醒、建議和指令 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-5 | 安全提醒、建議和指令 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-5 | 安全提醒、建議和指令 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-5 | 安全提醒、建議和指令 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI-12 | 資訊處理與保留 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12 | 資訊處理與保留 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays （Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| SI-12 | 資訊處理與保留 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12 | 資訊處理與保留 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 資訊處理與保留 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12 | 資訊處理與保留 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 資訊處理與保留 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12 | 資訊處理與保留 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 資訊處理與保留 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12 | 資訊處理與保留 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SI-12 | 資訊處理與保留 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SI-12 | 資訊處理與保留 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12 | 資訊處理與保留 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| SI-12 | 資訊處理與保留 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| SI-16 | 記憶體保護 | ecs-task-definition-memory-hard-limit | 限制 Amazon Elastic Container Service (ECS) 容器的可用記憶體上限，可確保當容器遇到惡意存取時，資源用量不會遭到濫用。 |

## 範本

該模板可用於 GitHub：FedRAMP（低）的操作最佳實踐。

# FedRAMP (適中) 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了聯邦風險與授權管理計畫 (FedRAMP) 與 AWS 受管 Config 規則之間的範例對映。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 FedRAMP 控制項相關。一個 FedRAMP 控制項可以與多項 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

本一致性套件由 AWS 安全保證服務 LLC (AWS SAS) 驗證，該公司是由支付卡產業合格安全評估機構 (QSA)、HITRUST 認證共同安全框架從業人員 (CCSFP) 以及經過認證的合規專業人員組成的團隊，可為各種產業框架提供指導和評估。 AWS SAS 專業人員設計了此「一致性套件」，使客戶能夠與 FedRAMP 控制的子集保持一致。

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | | | 軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(3) | 資訊系統會自動為使用者停用 90 天未經使用的帳戶。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(3) | 資訊系統會自動為使用者停用 90 天未經使用的帳戶。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(7) | 組織：(a) 根據角色型存取配置 (按角色組織允許的資訊系統存取和權限)，建立並管理特殊權限使用者；(b) 監視特殊權限角色指派；以及 (c) 當特殊權限角色指派不再適用時採取 [指派: 組織定義的動作]。補充指導：特殊權限角色是指派給個人的組織定義角色，使這些個人得以執行一般使用者未獲授權執行的某些安全性相關功能。這些特殊權限角色包括金鑰管理、帳戶管理、網路和系統管理、資料庫管理以及 Web 管理。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(7) | 組織：(a) 根據角色型存取配置 (按角色組織允許的資訊系統存取和權限)，建立並管理特殊權限使用者；(b) 監視特殊權限角色指派；以及 (c) 當特殊權限角色指派不再適用時採取 [指派: 組織定義的動作]。補充指導：特殊權限角色是指派給個人的組織定義角色，使這些個人得以執行一般使用者未獲授權執行的某些安全性相關功能。這些特殊權限角色包括金鑰管理、帳戶管理、網路和系統管理、資料庫管理以及 Web 管理。 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(7) | 組織：(a) 根據角色型存取配置 (按角色組織允許的資訊系統存取和權限)，建立並管理特殊權限使用者；(b) 監視特殊權限角色指派；以及 (c) 當特殊權限角色指派不再適用時採取 [指派: 組織定義的動作]。補充指導：特殊權限角色是指派給個人的組織定義角色，使這些個人得以執行一般使用者未獲授權執行的某些安全性相關功能。這些特殊權限角色包括金鑰管理、帳戶管理、網路和系統管理、資料庫管理以及 Web 管理。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(7) | 組織：(a) 根據角色型存取配置 (按角色組織允許的資訊系統存取和權限)，建立並管理特殊權限使用者；(b) 監視特殊權限角色指派；以及 (c) 當特殊權限角色指派不再適用時採取 [指派: 組織定義的動作]。補充指導：特殊權限角色是指派給個人的組織定義角色，使這些個人得以執行一般使用者未獲授權執行的某些安全性相關功能。這些特殊權限角色包括金鑰管理、帳戶管理、網路和系統管理、資料庫管理以及 Web 管理。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(7) | 組織：(a) 根據角色型存取配置 (按角色組織允許的資訊系統存取和權限)，建立並管理特殊權限使用者；(b) 監視特殊權限角色指派；以及 (c) 當特殊權限角色指派不再適用時採取 [指派: 組織定義的動作]。補充指導：特殊權限角色是指派給個人的組織定義角色，使這些個人得以執行一般使用者未獲授權執行的某些安全性相關功能。這些特殊權限角色包括金鑰管理、帳戶管理、網路和系統管理、資料庫管理以及 Web 管理。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(7) | 組織：(a) 根據角色型存取配置 (按角色組織允許的資訊系統存取和權限)，建立並管理特殊權限使用者；(b) 監視特殊權限角色指派；以及 (c) 當特殊權限角色指派不再適用時採取 [指派: 組織定義的動作]。補充指導：特殊權限角色是指派給個人的組織定義角色，使這些個人得以執行一般使用者未獲授權執行的某些安全性相關功能。這些特殊權限角色包括金鑰管理、帳戶管理、網路和系統管理、資料庫管理以及 Web 管理。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(12)(a) | 組織：a. 監控 [指派: 組織定義的非典型用途] 的資訊系統帳戶。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2(12)(a) | 組織：a. 監控 [指派: 組織定義的非典型用途] 的資訊系統帳戶。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC-6(10) | 資訊系統可防止非特殊權限使用者執行特權功能，包括停用、規避或改變已實作的安全保護/對策。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(10) | 資訊系統可防止非特殊權限使用者執行特權功能，包括停用、規避或改變已實作的安全保護/對策。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6(10) | 資訊系統可防止非特殊權限使用者執行特權功能，包括停用、規避或改變已實作的安全保護/對策。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。授予使用者超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分獲得或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 判斷資訊系統能否稽核下列事件：成功與失敗的帳戶登入事件、帳戶管理事件、物件存取、政策變更、權限功能、程序追蹤及系統事件。對於 Web 應用程式：所有管理員活動、驗證檢查、授權檢查、資料刪除、資料存取、資料變更和權限變更。d. 決定要在資訊系統內稽核下列事件：[針對每個已識別的事件持續稽核已在 AU-2 a 中定義之可稽核事件的組織定義子集]。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-7(1) | 資訊系統會根據 [指派: 稽核記錄中的組織定義稽核欄位]，讓您能夠處理感興趣事件的稽核記錄。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-7(1) | 資訊系統會根據 [指派: 稽核記錄中的組織定義稽核欄位]，讓您能夠處理感興趣事件的稽核記錄。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-9(2) | 資訊系統至少每週一次，將稽核記錄備份到與所稽核系統或元件不同的實體系統或系統元件上。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| AU-9(2) | 資訊系統至少每週一次，將稽核記錄備份到與所稽核系統或元件不同的實體系統或系統元件上。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| AU-9 | 資訊系統會保護稽核資訊和稽核工具免於未經授權的存取、修改和刪除。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-9 | 資訊系統會保護稽核資訊和稽核工具免於未經授權的存取、修改和刪除。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| AU-9 | 資訊系統會保護稽核資訊和稽核工具免於未經授權的存取、修改和刪除。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密功能。 |
| AU-11 | 組織會保留至少 90 天的稽核記錄，以提供安全性事件 after-the-fact 調查的支援，以及符合法規和組織資訊保留要求。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時，CloudTrail 將在新區域中建立相同的軌跡。因此，您將收到包含新區域 API 活動的日誌檔，而無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-12(a)(c) | 資訊系統：a. 在已部署/提供稽核功能的所有資訊系統與網路元件中，為 AU-2 a. 中定義的可稽核事件提供稽核記錄產生功能 c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳號 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可防止儲存貯體層級的公開存取，協助保護敏感資料的安全，免受未經授權的遠端使用者存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| CM-7(a) | 組織：a. 將資訊系統設定為僅提供基本功能。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-7(a) | 組織：a. 將資訊系統設定為僅提供基本功能。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-7(a) | 組織：a. 將資訊系統設定為僅提供基本功能。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(1) | 組織會將資訊系統元件的庫存清單更新為元件安裝、移除和資訊系統更新完整作業之一環。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-8(1) | 組織會將資訊系統元件的庫存清單更新為元件安裝、移除和資訊系統更新完整作業之一環。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(3)(a) | 組織：a. 持續運用自動化機制，使用偵測延遲上限五分鐘的自動化機制，偵測資訊系統中是否存在未經授權的硬體、軟體和韌體元件 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-8(3)(a) | 組織：a. 持續運用自動化機制，使用偵測延遲上限五分鐘的自動化機制，偵測資訊系統中是否存在未經授權的硬體、軟體和韌體元件 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(3)(a) | 組織：a. 持續運用自動化機制，使用偵測延遲上限五分鐘的自動化機制，偵測資訊系統中是否存在未經授權的硬體、軟體和韌體元件 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM-8(3)(a) | 組織：a. 持續運用自動化機制，使用偵測延遲上限五分鐘的自動化機制，偵測資訊系統中是否存在未經授權的硬體、軟體和韌體元件 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 對資訊系統所包含的資訊執行系統層級備份 (每日增量備份；每週完整備份)。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| IA-2(1)(2) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(2) 資訊系統會針對非特殊權限帳戶的網路存取實作多重要素驗證。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1)(2) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(2) 資訊系統會針對非特殊權限帳戶的網路存取實作多重要素驗證。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| IA-2(1)(2) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(2) 資訊系統會針對非特殊權限帳戶的網路存取實作多重要素驗證。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1)(2) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(2) 資訊系統會針對非特殊權限帳戶的網路存取實作多重要素驗證。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-2(1) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA-2(1) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2 | 資訊系統可唯一識別和驗證組織使用者 (或代表組織使用者行事流程)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2 | 資訊系統可唯一識別和驗證組織使用者 (或代表組織使用者行事流程)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(1)(a)(d)(e) | 適用於密碼型驗證的資訊系統：a. 強制執行 [指派: 組織定義的區分大小寫、字元數，以及混合大小寫字母、數字和特殊字元 (包括每種類型的最低要求) 要求] 的最低密碼複雜性；d. 強制執行 [指派: 組織定義的存留期上下限數值] 的密碼存留期上下限；e. 24 代內禁止重複使用相同密碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(4) | 組織運用自動化工具來判斷密碼驗證器的強度是否足以滿足 [指派: 組織定義的需求]。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(7) | 組織要確保未加密的靜態驗證器不會嵌入應用程式或存取指令碼中，也不會儲存在功能鍵上。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| IR-4(1) | 組織會運用自動化機制為事件處理流程提供支援。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-4(1) | 組織會運用自動化機制為事件處理流程提供支援。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| IR-4(1) | 組織會運用自動化機制為事件處理流程提供支援。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-4(1) | 組織會運用自動化機制為事件處理流程提供支援。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-4(1) | 組織會運用自動化機制為事件處理流程提供支援。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| IR-6(1) | 組織會運用自動化機制協助報告安全事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-6(1) | 組織會運用自動化機制協助報告安全事件。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-6(1) | 組織會運用自動化機制協助報告安全事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| IR-7(1) | 組織會運用自動化機制提高事件回應相關資訊和支援的可用性。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-7(1) | 組織會運用自動化機制提高事件回應相關資訊和支援的可用性。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-7(1) | 組織會運用自動化機制提高事件回應相關資訊和支援的可用性。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| RA-5(1) | 組織運用的漏洞掃描工具包括立即更新待掃描資訊系統漏洞的功能。補充指導：當發現並宣布新的漏洞以及開發出掃描方法時，需要立即更新待掃描的漏洞。此更新程序有助於確保儘快識別和解決資訊系統中的潛在漏洞。相關控制項：SI-3、SI-7。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| RA-5(1) | 組織運用的漏洞掃描工具包括立即更新待掃描資訊系統漏洞的功能。補充指導：當發現並宣布新的漏洞以及開發出掃描方法時，需要立即更新待掃描的漏洞。此更新程序有助於確保儘快識別和解決資訊系統中的潛在漏洞。相關控制項：SI-3、SI-7。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| RA-5(1) | 組織運用的漏洞掃描工具包括立即更新待掃描資訊系統漏洞的功能。補充指導：當發現並宣布新的漏洞以及開發出掃描方法時，需要立即更新待掃描的漏洞。此更新程序有助於確保儘快識別和解決資訊系統中的潛在漏洞。相關控制項：SI-3、SI-7。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| RA-5 | 組織：a. 每月掃描資訊系統及託管應用程式的漏洞 [作業系統/基礎設施; 每月 Web 應用程式及資料庫]，以及發現及報告可能影響系統/應用程式的新漏洞時；b. 運用可促進工具間互通性的漏洞掃描工具和技術，並使用以下標準將漏洞管理程序各部分自動化：1. 列舉平台、軟體缺陷和不正確的組態；2. 格式化檢查清單和測試程序；以及 3. 衡量漏洞影響；c. 分析漏洞掃描報告和安全控制評估的結果；d. 修補合法漏洞：依組織風險評估為據，自發現日起三十 (30) 天內緩解的高風險漏洞；自發現日起九十 (90) 天內緩解的中度風險漏洞；以及自發現日起一百八十 (180) 天內緩解的低風險漏洞；以及 e. 與 [指派: 組織定義的人員或角色] 共用從漏洞掃描程序和安全控制評估取得的資訊，以協助消除其他資訊系統 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 中的類似漏洞 (即系統弱點或缺陷)。 | | |
| RA-5 | 組織：a. 掃描資訊系統和託管應用程式中的漏洞 [指派: 組織定義的頻率和/或根據組織定義的程序隨機排列]，以及發現並報告可能影響系統/應用程式的新漏洞時；b. 運用可促進工具間互通性的漏洞掃描工具和技術，並使用以下標準將漏洞管理程序各部分自動化：1. 列舉平台、軟體缺陷和不正確的組態；2. 格式化檢查清單和測試程序；以及 3. 衡量漏洞影響；c. 分析漏洞掃描報告和安全控制評估的結果；d. 依組織的風險評估為據，修補合法漏洞 [指派: 組織定義的回應時間]；以及 e. 與 [指派: 組織定義的人員或角色] 共用從漏洞掃描程序和安全控制評估取得的資訊，以協助消除其他資訊系統中的類似漏洞 (即系統弱點或缺陷)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-3(a) | 組織：a. 使用包含資訊安全考量的 [指派: 組織定義的系統開發生命週期] 管理資訊系統。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SA-3(a) | 組織：a. 使用包含資訊安全考量的 [指派: 組織定義的系統開發生命週期] 管理資訊系統。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-3(a) | 組織：a. 使用包含資訊安全考量的 [指派: 組織定義的系統開發生命週期] 管理資訊系統。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務開發、實作和操作期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務開發、實作和操作期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務開發、實作和操作期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務開發、實作和操作期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-2 | 資訊系統會將使用者功能 (包括使用者介面服務) 與資訊系統管理功能分開。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| SC-2 | 資訊系統會將使用者功能 (包括使用者介面服務) 與資訊系統管理功能分開。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| SC-2 | 資訊系統會將使用者功能 (包括使用者介面服務) 與資訊系統管理功能分開。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-2 | 資訊系統會將使用者功能 (包括使用者介面服務) 與資訊系統管理功能分開。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| SC-2 | 資訊系統會將使用者功能 (包括使用者介面服務) 與資訊系統管理功能分開。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的爭用，為 Amazon EBS 磁碟區提供最有效率的效能。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7(4) | 組織：(a) 實作每項外部電信服務的受管介面；(b) 建立每個受管介面的流量政策；(c) 保護跨每個介面傳輸的資訊機密性和完整性；(d) 記錄流量政策的每個例外狀況，並附帶支援的任務/業務需求和該需求的持續時間；以及 (e) 檢閱流量政策 [指派: 組織定義的頻率] 的例外狀況，並移除明確任務/業務需求不再支援的例外狀況。補充指導：相關控制項：SC-8。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 組織：(a) 實作每項外部電信服務的受管介面；(b) 建立每個受管介面的流量政策；(c) 保護跨每個介面傳輸的資訊機密性和完整性；(d) 記錄流量政策的每個例外狀況，並附帶支援的任務/業務需求和該需求的持續時間；以及 (e) 檢閱流量政策 [指派: 組織定義的頻率] 的例外狀況，並移除明確任務/業務需求不再支援的例外狀況。補充指導：相關控制項：SC-8。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 組織：(a) 實作每項外部電信服務的受管介面；(b) 建立每個受管介面的流量政策；(c) 保護跨每個介面傳輸的資訊機密性和完整性；(d) 記錄流量政策的每個例外狀況，並附帶支援的任務/業務需求和該需求的持續時間；以及 (e) 檢閱流量政策 [指派: 組織定義的頻率] 的例外狀況，並移除明確任務/業務需求不再支援的例外狀況。補充指導：相關控制項：SC-8。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 組織：(a) 實作每項外部電信服務的受管介面；(b) 建立每個受管介面的流量政策；(c) 保護跨每個介面傳輸的資訊機密性和完整性；(d) 記錄流量政策的每個例外狀況，並附帶支援的任務/業務需求和該需求的持續時間；以及 (e) 檢閱流量政策 [指派: 組織定義的頻率] 的例外狀況，並移除明確任務/業務需求不再支援的例外狀況。補充指導：相關控制項：SC-8。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 組織：(a) 實作每項外部電信服務的受管介面；(b) 建立每個受管介面的流量政策；(c) 保護跨每個介面傳輸的資訊機密性和完整性；(d) 記錄流量政策的每個例外狀況，並附帶支援的任務/業務需求和該需求的持續時間；以及 (e) 檢閱流量政策 [指派: 組織定義的頻率] 的例外狀況，並移除明確任務/業務需求不再支援的例外狀況。補充指導：相關控制項：SC-8。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 組織：(a) 實作每項外部電信服務的受管介面；(b) 建立每個受管介面的流量政策；(c) 保護跨每個介面傳輸的資訊機密性和完整性；(d) 記錄流量政策的每個例外狀況，並附帶支援的任務/業務需求和該需求的持續時間；以及 (e) 檢閱流量政策 [指派: 組織定義的頻率] 的例外狀況，並移除明確任務/業務需求不再支援的例外狀況。補充指導：相關控制項：SC-8。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-7(5) | 受管介面的資訊系統預設拒絕網路通訊流量，但依例外狀況允許網路通訊流量 (即全部拒絕、依例外狀況允許)。補充指導：此控制增強功能適用於傳入和傳出網路通訊流量。拒絕全部 permit-by-exception 網路通訊流量政策可確保只允許那些必要且經過核准的連線。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的機密性和完整性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的機密性和完整性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8 | 資訊系統保護所傳輸資訊的機密性和完整性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的機密性和完整性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的機密性和完整性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-8 | 資訊系統保護所傳輸資訊的機密性和完整性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8 | 資訊系統保護所傳輸資訊的機密性和完整性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-12 | 組織根據 [指派: 組織定義的金鑰產成、分配、儲存、存取和銷毀要求] 為資訊系統中使用的必要密碼編譯建立及管理密碼編譯金鑰。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC-12 | 組織根據 [指派: 組織定義的金鑰產成、分配、儲存、存取和銷毀要求] 為資訊系統中使用的必要密碼編譯建立及管理密碼編譯金鑰。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-12 | 組織根據 [指派: 組織定義的金鑰產成、分配、儲存、存取和銷毀要求] 為資訊系統中使用的必要密碼編譯建立及管理密碼編譯金鑰。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作經 FIPS 驗證或 NSA 核准的密碼學。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作經 FIPS 驗證或 NSA 核准的密碼學。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作經 FIPS 驗證或 NSA 核准的密碼學。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作經 FIPS 驗證或 NSA 核准的密碼學。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作經 FIPS 驗證或 NSA 核准的密碼學。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作經 FIPS 驗證或 NSA 核准的密碼學。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密功能。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的機密性和完整性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(2) | 組織至少每月使用一次自動化機制，判斷與修補瑕疵有關的資訊系統元件狀態。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SI-2(2) | 組織至少每月使用一次自動化機制，判斷與修補瑕疵有關的資訊系統元件狀態。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(2) | 組織至少每月使用一次自動化機制，判斷與修補瑕疵有關的資訊系統元件狀態。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SI-2(2) | 組織至少每月使用一次自動化機制，判斷與修補瑕疵有關的資訊系統元件狀態。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3 | 組織：a. 在資訊系統進入點和退出點使用惡意程式碼保護機制，以偵測並消滅惡意程式碼；b. 根據組織組態管理政策和程序，一有新版本可用，即更新惡意程式碼保護機制；c. 將惡意程式碼保護機制設定為：1. 根據組織安全政策下載、開啟或執行檔案時，定期掃描資訊系統 [指派: 組織定義的頻率]，以及即時掃瞄 [選取項目 (一個或多個)、端點、網路進入點/退出點] 外部來源的檔案；以及 2. [選取項目 (一個或多個): 封鎖惡意程式碼; 隔離惡意程式碼; 向管理員傳送警示; [指派: 組織定義的動作]] 以回應惡意程式碼；以及 d. 解決偵測和消滅惡意程式碼期間收到的誤報，以及對資訊系統可用性造成的潛在影響。補充指導：資訊系統進入點和退出點包括防火牆、電子郵件伺服器、網 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 頁伺服器、Proxy 伺服器、遠端存取伺服器、工作站、筆記型電腦和行動裝置。惡意程式碼包括病毒、蠕蟲、Trojan 木馬程式和間諜軟體。惡意程式碼也可以使用各種格式（例如 UUENCODE、Unicode）進行編碼、包含在壓縮或隱藏檔案中，或使用隱寫法隱藏在檔案中。惡意程式碼可以透過不同的方式傳輸，例如網頁存取、電子郵件、電子郵件附件和可攜式儲存裝置。惡意程式碼是在惡意探索資訊系統漏洞時所插入。惡意程式碼保護機制包括防毒軟體特徵定義和信譽評等技術等等。有多種技術和方法可限制或消滅惡意程式碼的作用。無所不在的組態管理和全面的軟體完整性控制或可有效阻擋執行未經授權的程式碼。除了商業 off-the-shelf 軟體之外，客製化軟體中也可能存在惡意程式碼。這 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 可能包括邏輯炸彈、後門以及可能會影響組織任務/業務功能的其他類型網絡攻擊等等。傳統的惡意程式碼保護機制無法每次都偵測到此類程式碼。在這些情況下，組織就要仰賴其他保護措施，例如安全編碼實務、組態管理與控制、可信任的採購程序，以及監控實務，以協助確保軟體不會執行預期外的功能。組織可能會決定以不同的行動回應偵測到的惡意程式碼。例如，組織可以定義於定期掃描時偵測到惡意程式碼的回應動作、偵測到惡意下載時的回應動作，及/或嘗試開啟或執行檔案時偵測到惡意程式碼的回應動作。相關控制項：CM-3、MP-2、SA-4、SA-8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。參考文 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 獻：NIST 特別出版物 800-83。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3 | 組織：a. 在資訊系統進入點和退出點使用惡意程式碼保護機制，以偵測並消滅惡意程式碼；b. 根據組織組態管理政策和程序，一有新版本可用，即更新惡意程式碼保護機制；c. 將惡意程式碼保護機制設定為：1. 根據組織安全政策下載、開啟或執行檔案時，定期掃描資訊系統 [指派: 組織定義的頻率]，以及即時掃瞄 [選取項目 (一個或多個)、端點、網路進入點/退出點] 外部來源的檔案；以及 2. [選取項目 (一個或多個): 封鎖惡意程式碼; 隔離惡意程式碼; 向管理員傳送警示; [指派: 組織定義的動作]] 以回應惡意程式碼；以及 d. 解決偵測和消滅惡意程式碼期間收到的誤報，以及對資訊系統可用性造成的潛在影響。補充指導：資訊系統進入點和退出點包括防火牆、電子郵件伺服器、網 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 頁伺服器、Proxy 伺服器、遠端存取伺服器、工作站、筆記型電腦和行動裝置。惡意程式碼包括病毒、蠕蟲、Trojan 木馬程式和間諜軟體。惡意程式碼也可以使用各種格式（例如 UUENCODE、Unicode）進行編碼、包含在壓縮或隱藏檔案中，或使用隱寫法隱藏在檔案中。惡意程式碼可以透過不同的方式傳輸，例如網頁存取、電子郵件、電子郵件附件和可攜式儲存裝置。惡意程式碼是在惡意探索資訊系統漏洞時所插入。惡意程式碼保護機制包括防毒軟體特徵定義和信譽評等技術等等。有多種技術和方法可限制或消滅惡意程式碼的作用。無所不在的組態管理和全面的軟體完整性控制或可有效阻擋執行未經授權的程式碼。除了商業 off-the-shelf 軟體之外，客製化軟體中也可能存在惡意程式碼。這 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 可能包括邏輯炸彈、後門以及可能會影響組織任務/業務功能的其他類型網絡攻擊等等。傳統的惡意程式碼保護機制無法每次都偵測到此類程式碼。在這些情況下，組織就要仰賴其他保護措施，例如安全編碼實務、組態管理與控制、可信任的採購程序，以及監控實務，以協助確保軟體不會執行預期外的功能。組織可能會決定以不同的行動回應偵測到的惡意程式碼。例如，組織可以定義於定期掃描時偵測到惡意程式碼的回應動作、偵測到惡意下載時的回應動作，及/或嘗試開啟或執行檔案時偵測到惡意程式碼的回應動作。相關控制項：CM-3、MP-2、SA-4、SA-8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。參考文 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 獻：NIST 特別出版物 800-83。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3 | 組織：a. 在資訊系統進入點和退出點使用惡意程式碼保護機制，以偵測並消滅惡意程式碼；b. 根據組織組態管理政策和程序，一有新版本可用，即更新惡意程式碼保護機制；c. 將惡意程式碼保護機制設定為：1. 根據組織安全政策下載、開啟或執行檔案時，定期掃描資訊系統 [指派: 組織定義的頻率]，以及即時掃瞄 [選取項目 (一個或多個)、端點、網路進入點/退出點] 外部來源的檔案；以及 2. [選取項目 (一個或多個): 封鎖惡意程式碼; 隔離惡意程式碼; 向管理員傳送警示; [指派: 組織定義的動作]] 以回應惡意程式碼；以及 d. 解決偵測和消滅惡意程式碼期間收到的誤報，以及對資訊系統可用性造成的潛在影響。補充指導：資訊系統進入點和退出點包括防火牆、電子郵件伺服器、網 | ecs-task-definition-memory-hard-limit | 限制 Amazon Elastic Container Service (ECS) 容器的可用記憶體上限，可確保當容器遇到惡意存取時，資源用量不會遭到濫用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 頁伺服器、Proxy 伺服器、遠端存取伺服器、工作站、筆記型電腦和行動裝置。惡意程式碼包括病毒、蠕蟲、Trojan 木馬程式和間諜軟體。惡意程式碼也可以使用各種格式（例如 UUENCODE、Unicode）進行編碼、包含在壓縮或隱藏檔案中，或使用隱寫法隱藏在檔案中。惡意程式碼可以透過不同的方式傳輸，例如網頁存取、電子郵件、電子郵件附件和可攜式儲存裝置。惡意程式碼是在惡意探索資訊系統漏洞時所插入。惡意程式碼保護機制包括防毒軟體特徵定義和信譽評等技術等等。有多種技術和方法可限制或消滅惡意程式碼的作用。無所不在的組態管理和全面的軟體完整性控制或可有效阻擋執行未經授權的程式碼。除了商業 off-the-shelf 軟體之外，客製化軟體中也可能存在惡意程式碼。這 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 可能包括邏輯炸彈、後門以及可能會影響組織任務/業務功能的其他類型網絡攻擊等等。傳統的惡意程式碼保護機制無法每次都偵測到此類程式碼。在這些情況下，組織就要仰賴其他保護措施，例如安全編碼實務、組態管理與控制、可信任的採購程序，以及監控實務，以協助確保軟體不會執行預期外的功能。組織可能會決定以不同的行動回應偵測到的惡意程式碼。例如，組織可以定義於定期掃描時偵測到惡意程式碼的回應動作、偵測到惡意下載時的回應動作，及/或嘗試開啟或執行檔案時偵測到惡意程式碼的回應動作。相關控制項：CM-3、MP-2、SA-4、SA-8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。參考文 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 獻：NIST 特別出版物 800-83。 | | |
| SI-4(1) | 組織會將個別的入侵偵測工具連入全資訊系統的入侵偵測系統，並加以設定。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(4) | 資訊系統會持續監控傳入和傳出通訊流量，是否有異常或未經授權的活動或狀況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI-4(4) | 資訊系統會持續監控傳入和傳出通訊流量，是否有異常或未經授權的活動或狀況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(4) | 資訊系統會持續監控傳入和傳出通訊流量，是否有異常或未經授權的活動或狀況。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4(4) | 資訊系統會持續監控傳入和傳出通訊流量，是否有異常或未經授權的活動或狀況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-5 | 組織：a. 持續接收來自 [指派: 組織定義的外部組織] 的資訊系統安全警示、建議和指令；b. 視需要產生內部安全警示、建議和指令；c. 將安全警示、建議和指令散佈至：[選取項目 (一或多個): [指派: 組織定義的人員或角色]、[指派: 組織內的組織定義元素]、[指派: 組織定義的外部組織]]；以及 d. 按照既定的時間範圍實作安全指令，或通知核發機構不合規的程度。補充指導：美國電腦緊急應變小組 (US-CERT) 會產生安全警示和建議，以維持整個聯邦政府的情境意識。安全指令由 OMB 或其他負責發出此類指令的指定機構發出。安全指令必須遵守，因為這些指令有許多極其重要，若不及時實作，可能會對組織運作和資產、個人、其他組織和國家/地區立即產生不利的影響。外部組織包括外部任務/業 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 務合作夥伴、供應鏈合作夥伴、外部服務提供者，以及其他同行/支持組織等等。相關控制項：SI-2。參考文獻：NIST 特別出版物 800-40。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-5 | 組織：a. 持續接收來自 [指派: 組織定義的外部組織] 的資訊系統安全警示、建議和指令；b. 視需要產生內部安全警示、建議和指令；c. 將安全警示、建議和指令散佈至：[選取項目 (一或多個): [指派: 組織定義的人員或角色]、[指派: 組織內的組織定義元素]、[指派: 組織定義的外部組織]]；以及 d. 按照既定的時間範圍實作安全指令，或通知核發機構不合規的程度。補充指導：美國電腦緊急應變小組 (US-CERT) 會產生安全警示和建議，以維持整個聯邦政府的情境意識。安全指令由 OMB 或其他負責發出此類指令的指定機構發出。安全指令必須遵守，因為這些指令有許多極其重要，若不及時實作，可能會對組織運作和資產、個人、其他組織和國家/地區立即產生不利的影響。外部組織包括外部任務/業 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 務合作夥伴、供應鏈合作夥伴、外部服務提供者，以及其他同行/支持組織等等。相關控制項：SI-2。參考文獻：NIST 特別出版物 800-40。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-5 | 組織：a. 持續接收來自 [指派: 組織定義的外部組織] 的資訊系統安全警示、建議和指令；b. 視需要產生內部安全警示、建議和指令；c. 將安全警示、建議和指令散佈至：[選取項目 (一或多個): [指派: 組織定義的人員或角色]、[指派: 組織內的組織定義元素]、[指派: 組織定義的外部組織]]；以及 d. 按照既定的時間範圍實作安全指令，或通知核發機構不合規的程度。補充指導：美國電腦緊急應變小組 (US-CERT) 會產生安全警示和建議，以維持整個聯邦政府的情境意識。安全指令由 OMB 或其他負責發出此類指令的指定機構發出。安全指令必須遵守，因為這些指令有許多極其重要，若不及時實作，可能會對組織運作和資產、個人、其他組織和國家/地區立即產生不利的影響。外部組織包括外部任務/業 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 務合作夥伴、供應鏈合作夥伴、外部服務提供者，以及其他同行/支持組織等等。相關控制項：SI-2。參考文獻：NIST 特別出版物 800-40。 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-5 | 組織：a. 持續接收來自 [指派: 組織定義的外部組織] 的資訊系統安全警示、建議和指令；b. 視需要產生內部安全警示、建議和指令；c. 將安全警示、建議和指令散佈至：[選取項目 (一或多個): [指派: 組織定義的人員或角色]、[指派: 組織內的組織定義元素]、[指派: 組織定義的外部組織]]；以及 d. 按照既定的時間範圍實作安全指令，或通知核發機構不合規的程度。補充指導：美國電腦緊急應變小組 (US-CERT) 會產生安全警示和建議，以維持整個聯邦政府的情境意識。安全指令由 OMB 或其他負責發出此類指令的指定機構發出。安全指令必須遵守，因為這些指令有許多極其重要，若不及時實作，可能會對組織運作和資產、個人、其他組織和國家/地區立即產生不利的影響。外部組織包括外部任務/業 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | 務合作夥伴、供應鏈合作夥伴、外部服務提供者，以及其他同行/支持組織等等。相關控制項：SI-2。參考文獻：NIST 特別出版物 800-40。 | | |
| SI-7(1) | 資訊系統至少每月執行一次完整性檢查安全相關事件。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(1) | 資訊系統至少每月執行一次完整性檢查安全相關事件。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SI-7(1) | 資訊系統至少每月執行一次完整性檢查安全相關事件。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7 | 組織會使用完整性驗證工具來偵測 [指派: 組織定義的軟體、韌體和資訊] 的未經授權變更。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-11 | 資訊系統：a. 產生可為修正動作提供所需資訊的錯誤訊息，但不會洩漏可能遭攻擊者利用的資訊；以及 b. 僅向 [指派: 組織定義的人員或角色] 顯示錯誤訊息。補充指導：組織要仔細考慮錯誤訊息的結構/內容。資訊系統能夠識別和處理錯誤狀況的程度，是由組織政策和營運需求所引導。攻擊者可能利用的資訊包括：不小心在使用者名稱中輸入密碼的錯誤登入嘗試、可由所記錄資訊 (如果未明確說明) 衍生的任務/商業資訊，以及個人資訊，例如帳號、社會安全號碼和信用卡號碼等等。此外，錯誤訊息可能會提供隱蔽通道用以傳輸資訊。相關控制項：AU-2、AU-3、SC-31。控制增強功能：無。參考：無。 | [api-gw-execution-logging-enabled](https://) | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-11 | 資訊系統：a. 產生可為修正動作提供所需資訊的錯誤訊息，但不會洩漏可能遭攻擊者利用的資訊；以及 b. 僅向 [指派: 組織定義的人員或角色] 顯示錯誤訊息。補充指導：組織要仔細考慮錯誤訊息的結構/內容。資訊系統能夠識別和處理錯誤狀況的程度，是由組織政策和營運需求所引導。攻擊者可能利用的資訊包括：不小心在使用者名稱中輸入密碼的錯誤登入嘗試、可由所記錄資訊 (如果未明確說明) 衍生的任務/商業資訊，以及個人資訊，例如帳號、社會安全號碼和信用卡號碼等等。此外，錯誤訊息可能會提供隱蔽通道用以傳輸資訊。相關控制項：AU-2、AU-3、SC-31。控制增強功能：無。參考：無。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-11 | 資訊系統：a. 產生可為修正動作提供所需資訊的錯誤訊息，但不會洩漏可能遭攻擊者利用的資訊；以及 b. 僅向 [指派: 組織定義的人員或角色] 顯示錯誤訊息。補充指導：組織要仔細考慮錯誤訊息的結構/內容。資訊系統能夠識別和處理錯誤狀況的程度，是由組織政策和營運需求所引導。攻擊者可能利用的資訊包括：不小心在使用者名稱中輸入密碼的錯誤登入嘗試、可由所記錄資訊 (如果未明確說明) 衍生的任務/商業資訊，以及個人資訊，例如帳號、社會安全號碼和信用卡號碼等等。此外，錯誤訊息可能會提供隱蔽通道用以傳輸資訊。相關控制項：AU-2、AU-3、SC-31。控制增強功能：無。參考：無。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-11 | 資訊系統：a. 產生可為修正動作提供所需資訊的錯誤訊息，但不會洩漏可能遭攻擊者利用的資訊；以及 b. 僅向 [指派: 組織定義的人員或角色] 顯示錯誤訊息。補充指導：組織要仔細考慮錯誤訊息的結構/內容。資訊系統能夠識別和處理錯誤狀況的程度，是由組織政策和營運需求所引導。攻擊者可能利用的資訊包括：不小心在使用者名稱中輸入密碼的錯誤登入嘗試、可由所記錄資訊 (如果未明確說明) 衍生的任務/商業資訊，以及個人資訊，例如帳號、社會安全號碼和信用卡號碼等等。此外，錯誤訊息可能會提供隱蔽通道用以傳輸資訊。相關控制項：AU-2、AU-3、SC-31。控制增強功能：無。參考：無。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-11 | 資訊系統：a. 產生可為修正動作提供所需資訊的錯誤訊息，但不會洩漏可能遭攻擊者利用的資訊；以及 b. 僅向 [指派: 組織定義的人員或角色] 顯示錯誤訊息。補充指導：組織要仔細考慮錯誤訊息的結構/內容。資訊系統能夠識別和處理錯誤狀況的程度，是由組織政策和營運需求所引導。攻擊者可能利用的資訊包括：不小心在使用者名稱中輸入密碼的錯誤登入嘗試、可由所記錄資訊 (如果未明確說明) 衍生的任務/商業資訊，以及個人資訊，例如帳號、社會安全號碼和信用卡號碼等等。此外，錯誤訊息可能會提供隱蔽通道用以傳輸資訊。相關控制項：AU-2、AU-3、SC-31。控制增強功能：無。參考：無。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-11 | 資訊系統：a. 產生可為修正動作提供所需資訊的錯誤訊息，但不會洩漏可能遭攻擊者利用的資訊；以及 b. 僅向 [指派: 組織定義的人員或角色] 顯示錯誤訊息。補充指導：組織要仔細考慮錯誤訊息的結構/內容。資訊系統能夠識別和處理錯誤狀況的程度，是由組織政策和營運需求所引導。攻擊者可能利用的資訊包括：不小心在使用者名稱中輸入密碼的錯誤登入嘗試、可由所記錄資訊 (如果未明確說明) 衍生的任務/商業資訊，以及個人資訊，例如帳號、社會安全號碼和信用卡號碼等等。此外，錯誤訊息可能會提供隱蔽通道用以傳輸資訊。相關控制項：AU-2、AU-3、SC-31。控制增強功能：無。參考：無。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-11 | 資訊系統：a. 產生可為修正動作提供所需資訊的錯誤訊息，但不會洩漏可能遭攻擊者利用的資訊；以及 b. 僅向 [指派: 組織定義的人員或角色] 顯示錯誤訊息。補充指導：組織要仔細考慮錯誤訊息的結構/內容。資訊系統能夠識別和處理錯誤狀況的程度，是由組織政策和營運需求所引導。攻擊者可能利用的資訊包括：不小心在使用者名稱中輸入密碼的錯誤登入嘗試、可由所記錄資訊 (如果未明確說明) 衍生的任務/商業資訊，以及個人資訊，例如帳號、社會安全號碼和信用卡號碼等等。此外，錯誤訊息可能會提供隱蔽通道用以傳輸資訊。相關控制項：AU-2、AU-3、SC-31。控制增強功能：無。參考：無。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-16 | 資訊系統實作 [指派: 組織定義的安全防護]，保護記憶體免於未經授權的程式碼執行。補充指導：有些攻擊者發動攻擊的目的是為了在記憶體的非可執行區域或禁止的記憶體位置中執行程式碼。用以保護記憶體的安全保護包括防止資料執行和位址空間配置隨機化等等。您可以在硬體上運用硬體或軟體方式強制執行防止資料執行的防護措施，以提供更強大的機制。相關控制項：AC-25、SC-3。控制增強功能：無。參考：無。 | ecs-task-definition-memory-hard-limit | 限制 Amazon Elastic Container Service (ECS) 容器的可用記憶體上限，可確保當容器遇到惡意存取時，資源用量不會遭到濫用。 |

### 範本

該模板可在以下位置獲得 GitHub：FedRAMP 的操作最佳實踐（中等）。

## FFIEC 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了聯邦金融機構考試委員會（FFIEC）網絡安全評估工具域和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 FFIEC 網路安全評估工具控制

項相關。FFIEC 網路安全評定工具控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.G.IT.B.1 | 系統會維護組織資產清單 (例如硬體、軟體、資料和外部託管的系統)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| D1.G.IT.B.1 | 系統會維護組織資產清單 (例如硬體、軟體、資料和外部託管的系統)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| D1.G.IT.B.1 | 系統會維護組織資產清單 (例如硬體、軟體、資料和外部託管的系統)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| D1.G.IT.B.1 | 系統會維護組織資產清單 (例如硬體、軟體、資料和外部託管的系統)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | 此機構內存在資訊安全及業務持續性風險管理功能。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| D1.RM.RA.B.2 | 風險評定可識別需要額外驗證控制的網際網路型系統和高風險交易。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| D1.RM.RA.B.2 | 風險評定可識別需要額外驗證控制的網際網路型系統和高風險交易。 | annual-risk-assessment-performed（過程檢查） | 對貴組織執行年度風險評估。風險評定可協助判定已識別風險和/或漏洞影響組織的可能性及影響。 |
| D1.TC.Tr.B.2 | 年度資訊安全訓練包括事件回應、目前的網路威脅 (例如網路釣魚、魚叉式網路釣魚、社交工程和行動安全)，以及新出現的問題。 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計畫可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.IS.Is.B.1 | 收集資訊安全威脅並與適當的內部員工共用。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| D2.IS.Is.B.1 | 收集資訊安全威脅並與適當的內部員工共用。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| D2.IS.Is.B.1 | 收集資訊安全威脅並與適當的內部員工共用。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能靜態存在敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | cw-loggroup-retent ion-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | 以安全的方式檢閱並保留稽核日誌記錄和其他安全事件日誌。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | redshift-cluster-c onfiguration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Con fig 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | 電腦事件記錄檔會在事件發生後用於調查。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| D2.TI.Ti.B.1 | 該機構屬於或訂閱威脅和漏洞資訊共享來源，該來源提供威脅相關資訊（例如 FS-ISAC、US-CERT）。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.TI.Ti.B.1 | 該機構屬於或訂閱威脅和漏洞資訊共享來源，該來源提供威脅相關資訊（例如 FS-ISAC、US-CERT）。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| D2.TI.Ti.B.2 | 將威脅資訊用於監控威脅和漏洞。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| D2.TI.Ti.B.2 | 將威脅資訊用於監控威脅和漏洞。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.TI.Ti.B.2 | 將威脅資訊用於監控威脅和漏洞。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D2.TI.Ti.B.3 | 將威脅資訊用於強化內部風險管理和控制。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| D2.TI.Ti.B.3 | 將威脅資訊用於強化內部風險管理和控制。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.CC.PM.B.1 | 實作修補程式管理計畫，並確保及時套用軟體和韌體修補程式。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| D3.CC.PM.B.1 | 實作修補程式管理計畫，並確保及時套用軟體和韌體修補程式。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| D3.CC.PM.B.1 | 實作修補程式管理計畫，並確保及時套用軟體和韌體修補程式。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.CC.PM.B.1 | 實作修補程式管理計畫，並確保及時套用軟體和韌體修補程式。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| D3.CC.PM.B.3 | 檢閱修補程式管理報告，該報告可反映缺少的安全修補程式。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.CC.PM.B.3 | 檢閱修補程式管理報告，該報告可反映缺少的安全修補程式。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| D3.CC.PM.B.3 | 檢閱修補程式管理報告，該報告可反映缺少的安全修補程式。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.CC.PM.B.3 | 檢閱修補程式管理報告，該報告可反映缺少的安全修補程式。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.1 | 此機構能夠透過監控整個環境來偵測異常活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.1 | 此機構能夠透過監控整個環境來偵測異常活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| D3.DC.An.B.1 | 此機構能夠透過監控整個環境來偵測異常活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.2 | 監控並檢閱產生異常活動提醒的客戶交易。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| D3.DC.An.B.2 | 監控並檢閱產生異常活動提醒的客戶交易。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | 在事件發生後檢閱實體和/或邏輯存取的日誌。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| D3.DC.An.B.4 | 監控第三方對關鍵系統的存取是否存在未經授權或異常活動 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| D3.DC.An.B.5 | 監控更高的權限。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.An.B.5 | 監控更高的權限。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| D3.DC.Ev.B.1 | 建立正常的網路活動基準。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.Ev.B.2 | 設有機制 (例如，防毒警示、記錄事件警示) 可用來警示管理潛在攻擊。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| D3.DC.Ev.B.3 | 施行程序來監控是否有未經授權的使用者、裝置、連線及軟體。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| D3.DC.Ev.B.3 | 施行程序來監控是否有未經授權的使用者、裝置、連線及軟體。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.Ev.B.3 | 施行程序來監控是否有未經授權的使用者、裝置、連線及軟體。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| D3.DC.Ev.B.3 | 施行程序來監控是否有未經授權的使用者、裝置、連線及軟體。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.Th.B.1 | 根據傳出系統和內部網路的風險評定進行獨立測試 (包括滲透測試和漏洞掃描)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| D3.DC.Th.B.1 | 根據傳出系統和內部網路的風險評定進行獨立測試 (包括滲透測試和漏洞掃描)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.DC.Th.B.1 | 根據傳出系統和內部網路的風險評定進行獨立測試 (包括滲透測試和漏洞掃描)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedAc tionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| D3.PC.Am.B.1 | 根據工作職責和最低權限的原則，將系統和機密資料的存取權授予員工。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.10 | 隔離生產環境和非生產環境，以防止未經授權存取或變更資訊資產。(*如果機構或機構的第三方沒有生產環境，則為不適用。) | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.10 | 隔離生產環境和非生產環境，以防止未經授權存取或變更資訊資產。(*如果機構或機構的第三方沒有生產環境，則為不適用。) | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| D3.PC.Am.B.10 | 隔離生產環境和非生產環境，以防止未經授權存取或變更資訊資產。(*如果機構或機構的第三方沒有生產環境，則為不適用。) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.10 | 隔離生產環境和非生產環境，以防止未經授權存取或變更資訊資產。(*如果機構或機構的第三方沒有生產環境，則為不適用。) | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| D3.PC.Am.B.12 | 在儲存和傳輸過程中加密所有密碼。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.13 | 機密資料在公用或不受信任的網路 (例如，網際網路) 傳輸時會加密。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| D3.PC.Am.B.13 | 機密資料在公用或不受信任的網路 (例如，網際網路) 傳輸時會加密。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.13 | 機密資料在公用或不受信任的網路 (例如，網際網路) 傳輸時會加密。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.13 | 機密資料在公用或不受信任的網路 (例如，網際網路) 傳輸時會加密。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.13 | 機密資料在公用或不受信任的網路 (例如，網際網路) 傳輸時會加密。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.13 | 機密資料在公用或不受信任的網路 (例如，網際網路) 傳輸時會加密。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.13 | 機密資料在公用或不受信任的網路 (例如，網際網路) 傳輸時會加密。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| D3.PC.Am.B.15 | 員工、承包商及第三方對關鍵系統的遠端存取使用加密連線和多重要素驗證。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.15 | 員工、承包商及第三方對關鍵系統的遠端存取使用加密連線和多重要素驗證。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.15 | 員工、承包商及第三方對關鍵系統的遠端存取使用加密連線和多重要素驗證。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| D3.PC.Am.B.15 | 員工、承包商及第三方對關鍵系統的遠端存取使用加密連線和多重要素驗證。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.15 | 員工、承包商及第三方對關鍵系統的遠端存取使用加密連線和多重要素驗證。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| D3.PC.Am.B.15 | 員工、承包商及第三方對關鍵系統的遠端存取使用加密連線和多重要素驗證。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| D3.PC.Am.B.15 | 員工、承包商及第三方對關鍵系統的遠端存取使用加密連線和多重要素驗證。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.16 | 施行管理、物理或技術控制，以防止沒有管理責任的使用者安裝未經授權的軟體。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Am.B.16 | 施行管理、物理或技術控制，以防止沒有管理責任的使用者安裝未經授權的軟體。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.16 | 施行管理、物理或技術控制，以防止沒有管理責任的使用者安裝未經授權的軟體。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Am.B.16 | 施行管理、物理或技術控制，以防止沒有管理責任的使用者安裝未經授權的軟體。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Am.B.2 | 員工對系統和機密資料的存取可提供職責分離。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.2 | 員工對系統和機密資料的存取可提供職責分離。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Am.B.2 | 員工對系統和機密資料的存取可提供職責分離。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Am.B.3 | 提升的權限 (例如管理員權限) 受到限制且受到嚴格控制 (例如，指派給個人、非共用，而且需要更強大的密碼控制) | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.3 | 提升的權限 (例如管理員權限) 受到限制且受到嚴格控制 (例如，指派給個人、非共用，而且需要更強大的密碼控制) | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| D3.PC.Am.B.3 | 提升的權限 (例如管理員權限) 受到限制且受到嚴格控制 (例如，指派給個人、非共用，而且需要更強大的密碼控制)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.3 | 提升的權限 (例如管理員權限) 受到限制且受到嚴格控制 (例如，指派給個人、非共用，而且需要更強大的密碼控制) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| D3.PC.Am.B.3 | 提升的權限 (例如管理員權限) 受到限制且受到嚴格控制 (例如，指派給個人、非共用，而且需要更強大的密碼控制) | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Am.B.3 | 提升的權限 (例如管理員權限) 受到限制且受到嚴格控制 (例如，指派給個人、非共用，而且需要更強大的密碼控制) | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| D3.PC.Am.B.6 | 系統、應用程式和硬體的存取需要識別和驗證，並對其進行管理。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.7 | 存取控制包括密碼複雜性以及密碼嘗試和重複使用的限制。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Am.B.8 | 在系統實作之前變更所有預設密碼和不必要的預設帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路界面的公有 IP 地址。 |
| D3.PC.Im.B.1 | 使用網路周邊防禦工具 (例如邊界路由器和防火牆)。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.2 | 透過防火牆或其他類似的裝置保護從網際網路或由外部各方存取的系統。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| D3.PC.IM.B.2 | 透過防火牆或其他類似的裝置保護從網際網路或由外部各方存取的系統。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.2 | 透過防火牆或其他類似的裝置保護從網際網路或由外部各方存取的系統。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| D3.PC.IM.B.2 | 透過防火牆或其他類似的裝置保護從網際網路或由外部各方存取的系統。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.2 | 透過防火牆或其他類似的裝置保護從網際網路或由外部各方存取的系統。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| D3.PC.IM.B.2 | 透過防火牆或其他類似的裝置保護從網際網路或由外部各方存取的系統。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.3 | 監控所有連接埠。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D3.PC.IM.B.3 | 監控所有連接埠。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| D3.PC.IM.B.3 | 監控所有連接埠。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.3 | 監控所有連接埠。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| D3.PC.IM.B.3 | 監控所有連接埠。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.3 | 監控所有連接埠。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| D3.PC.Im.B.5 | 系統組態 (適用於伺服器、桌上型電腦、路由器等) 遵循業界標準並予以強制執行 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.5 | 系統組態 (適用於伺服器、桌上型電腦、路由器等) 遵循業界標準並予以強制執行 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| D3.PC.Im.B.5 | 系統組態 (適用於伺服器、桌上型電腦、路由器等) 遵循業界標準並予以強制執行 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.6 | 如果不再需要用於商業目的，則禁止使用連接埠、功能、通訊協定及服務。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| D3.PC.IM.B.6 | 如果不再需要用於商業目的，則禁止使用連接埠、功能、通訊協定及服務。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.IM.B.6 | 如果不再需要用於商業目的，則禁止使用連接埠、功能、通訊協定及服務。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| D3.PC.IM.B.6 | 如果不再需要用於商業目的，則禁止使用連接埠、功能、通訊協定及服務。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.7 | 控制並監控對系統組態 (包括虛擬機器和 Hypervisor) 進行變更的存取。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Im.B.7 | 控制並監控對系統組態 (包括虛擬機器和 Hypervisor) 進行變更的存取。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| D3.PC.Im.B.7 | 控制並監控對系統組態 (包括虛擬機器和 Hypervisor) 進行變更的存取。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.7 | 控制並監控對系統組態 (包括虛擬機器和 Hypervisor) 進行變更的存取。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Im.B.7 | 控制並監控對系統組態 (包括虛擬機器和 Hypervisor) 進行變更的存取。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D3.PC.Im.B.7 | 控制並監控對系統組態 (包括虛擬機器和 Hypervisor) 進行變更的存取。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D3.PC.Im.B.7 | 控制並監控對系統組態 (包括虛擬機器和 Hypervisor) 進行變更的存取。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| D3.PC.Se.B.1 | 在此機構工作的開發人員遵循符合業界標準的安全程式編碼實務，作為系統開發生命週期 (SDLC) 的一部分。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| D3.PC.Se.B.1 | 在此機構工作的開發人員遵循符合業界標準的安全程式編碼實務，作為系統開發生命週期 (SDLC) 的一部分。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D4.C.Co.B.2 | 此機構確保第三方連線獲得授權。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| D4.C.Co.B.2 | 此機構確保第三方連線獲得授權。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D4.C.Co.B.2 | 此機構確保第三方連線獲得授權。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| D4.C.Co.B.2 | 此機構確保第三方連線獲得授權。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.1 | 設定提醒參數以便偵測提示緩解動作的資訊安全事件。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.1 | 設定提醒參數以便偵測提示緩解動作的資訊安全事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| D5.DR.De.B.1 | 設定提醒參數以便偵測提示緩解動作的資訊安全事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.2 | 系統效能報告包含的資訊可用作偵測資訊安全事件的風險指標 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| D5.DR.De.B.2 | 系統效能報告包含的資訊可用作偵測資訊安全事件的風險指標 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | 施行工具和程序來偵測、提醒及觸發事件回應程式。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.ER.Es.B.4 | 分類、記錄及追蹤事件。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| D5.IR.Pl.B.1 | 此機構已記載其將如何應對和回應網路事件。 | response-plan-exists-maintained （過程檢查） | 確保已建立、維護事件回應計畫，並將其分發給負責人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| D5.IR.PI.B.6 | 此機構規劃使用業務持續性、災難復原以及資料備份程式，在事件發生後復原操作。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。。 |

## 範本

該模板位於以下網站 GitHub：FFIEC 的營運最佳實踐。

# 德國雲端運算合規性標準目錄 (C5) 的最佳作業實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供德國雲端運算合規標準目錄 (C5) 和 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個德國 C5 控制項相關。德國 C5 控件可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 公司 -01 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 公司 -01 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 公司 -01 | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 公司 -01 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |
| 公司 -01 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| 公司 -01 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 科斯 -03 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 科斯 -03 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 科斯 -03 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 科斯 -03 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 科斯 -03 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 科斯 -03 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 科斯 -03 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 科斯 -03 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 科斯 -03 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 科斯 -03 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 科斯 -03 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 科斯 -03 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 科斯 -03 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 科斯 -03 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 科斯 -03 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 科斯 -03 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 科斯 -03 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 科斯 -03 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 科斯 -03 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 科斯 -03 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 科斯 -03 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 公司 -05 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 公司 -05 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 公司 -05 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 公司 -05 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 公司 -05 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 公司 -05 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 公司 -05 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 公司 -05 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 公司 -05 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 公司 -05 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 公司 -05 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 公司 -05 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 公司 -05 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 哭泣的 -02 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 哭泣的 -02 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 哭泣的 -02 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| 哭泣的 -02 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 哭泣的 -02 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 哭泣的 -02 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 哭泣的 -02 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 哭泣的 -02 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 哭泣的 -02 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 哭泣的同位素 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 哭泣的同位素 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 哭泣的同位素 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 哭泣的同位素 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 哭泣的同位素 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 哭泣的同位素 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 哭泣的同位素 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 哭泣的同位素 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 哭泣的同位素 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 哭泣的同位素 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 哭泣的同位素 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 哭泣的同位素 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 哭泣的同位素 | rds-snapshot-encrypted | 確保已針對 Amazon Relationa l Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 哭泣的同位素 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| 哭泣的同位素 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 哭泣的同位素 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 哭泣的同位素 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 哭泣的同位素 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 哭泣的同位素 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 哭泣的同位素 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 哭泣的 -04 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 開發 -07 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 開發 -07 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 開發 -07 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 開發 -07 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 開發 -07 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 開發 -07 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| IDM-01 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| IDM-01 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| IDM-01 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| IDM-01 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IDM-01 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IDM-01 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IDM-01 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| IDM-01 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| IDM-01 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| IDM-01 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| IDM-01 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| IDM-01 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| IDM-01 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |
| IDM-01 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| IDM-01 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-01 | rds-instance-iam-authentication-enabled | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體上啟用 AWS 身分和存取管理 (IAM) 身份驗證，以控制對系統和資產的存取。這會強制使用 Secure Sockets Layer (SSL) 來加密往返資料庫的網路流量。您不需要將使用者憑證放在資料庫，因為身分驗證是由外部管理。 |
| IDM-01 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| IDM-03 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-03 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |
| IDM-08 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| CRY-01 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| IDM-09 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| IDM-09 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IDM-09 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IDM-09 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-01 | clb-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| OPS-01 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| OPS-01 | lambda-vpc-multi-az-check | 如果您的 AWS Lambda 函數設定為連線到帳戶中的虛擬私有雲 (VPC)，請在至少兩個不同的可用區域中部署 AWS Lambda 函數，以確保在單一區域中發生服務中斷時，它是您的函數可用來處理事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-01 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| OPS-01 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-01 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| OPS-01 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| OPS-01 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-02 | clb-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| OPS-02 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| OPS-02 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-02 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| OPS-02 | lambda-vpc-multi-az-check | 如果您的 AWS Lambda 函數設定為連線到帳戶中的虛擬私有雲 (VPC)，請在至少兩個不同的可用區域中部署 AWS Lambda 函數，以確保在單一區域中發生服務中斷時，它是您的函數可用來處理事件。 |
| OPS-02 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-02 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| OPS-02 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| OPS-02 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-02 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| OPS-07 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-07 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| OPS-07 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| OPS-07 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-07 | opensearch-data-node-fault-tolerance | Amazon OpenSearch 服務 (服 OpenSearch 務) 至少需要三個資料節點才能達到高可用性和容錯能力。部署具有至少三個資料節點的 OpenSearch Service 網域可確保節點失敗時的叢集作業。 |
| OPS-07 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| OPS-07 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-07 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| OPS-07 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| OPS-07 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-07 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| OPS-07 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| OPS-07 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-07 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| OPS-07 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| OPS-12 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| OPS-12 | s3-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-13 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| OPS-13 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-13 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| OPS-14 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| OPS-14 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-14 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| OPS-14 | s3-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| OPS-15 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| OPS-15 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| OPS-15 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-15 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| OPS-15 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| OPS-15 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| OPS-15 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-15 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| OPS-15 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| OPS-15 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| OPS-15 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-15 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| OPS-15 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| OPS-15 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| OPS-15 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| OPS-15 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| OPS-22 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |
| PSS-05 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| PSS-05 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| PSS-05 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| PSS-05 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| PSS-07 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

### 範本

該模板可在以下網站獲得 GitHub：德國雲計算合規標準目錄（C5）。

## Gramm Leach Bliley Act (GLBA) 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 Gramm Leach Bliley Act (GLBA) 與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 GLBA 控制項相關。一個 GLBA 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Ama |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 受其司法管轄權管轄的金融機構訂立適當的標準 | | zon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| GLBA-SEC.501(b) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護方面，為受其司法管轄權管轄的金融機構訂立適當的標準 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| GLBA-SEC.501(b)(1) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (1) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以確保客戶記錄及資訊的安全與保密。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(2) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄之安全性或完整性所構成的預期威脅或危害；及 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| GLBA-SEC.501(b)(2) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄之安全性或完整性所構成的預期威脅或危害；及 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或任務職能將使用者放入群組中，是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| GLBA-SEC.501(b)(3) | 為推動 (a) 款內的政策，第 505(a) 條所述的每個機構或主管當局均須在行政、技術和物理防護 (2) 方面，為受其司法管轄權管轄的金融機構訂立適當的標準，以防範任何對這類記錄或資訊的未授權存取，其可能對任何客戶產生實質性的損害或困擾。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

## 範本

該模板可用於 GitHub：格蘭姆·利奇·布利利法案（GLBA）的操作最佳實踐。

# GxP EU Annex 11 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 GxP 歐盟附件 11 與 AWS 受管 Config 規則之間的對應範例。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 GxP EU 附件 11 控制項相關。一個 GxP EU Annex 11 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1. 風險管理 | 風險管理應考慮病患安全、資料完整性和產品品質，並套用到整個電腦化系統的生命週期中。作為風險管理系統的一部分，有關驗證範圍和資料完整性控制的決定應根據合理且已記載的電腦化系統風險評估。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 1. 風險管理 | 風險管理應考慮病患安全、資料完整性和產品品質，並套用到整個電腦化系統的生命週期中。作為風險管理系統的一部分，有關驗證範圍和資料完整性控制的決定應根據合理且已記載的電腦化系統風險評估。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 4.2. 驗證 - 文件變更控制 | 驗證文件應包含變更控制記錄 (如適用)，以及驗證程序期間觀察到任何偏離的報告。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.3. 驗證 - 庫存清單 | 應該提供所有相關系統及其 GMP 功能的最新清單 (庫存清單)。對於重要系統，應提供最新的系統描述，詳細說明實體和邏輯排列、與其他系統或程序之間的資料流程和介面、任何硬體和軟體先決條件以及安全措施。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 4.3. 驗證 - 庫存清單 | 應該提供所有相關系統及其 GMP 功能的最新清單 (庫存清單)。對於重要系統，應提供最新的系統描述，詳細說明實體和邏輯排列、與其他系統或程序之間的資料流程和介面、任何硬體和軟體先決條件以及安全措施。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.3. 驗證 - 庫存清單 | 應該提供所有相關系統及其 GMP 功能的最新清單 (庫存清單)。對於重要系統，應提供最新的系統描述，詳細說明實體和邏輯排列、與其他系統或程序之間的資料流程和介面、任何硬體和軟體先決條件以及安全措施。 | ec2-security-group-attached-to-eni-periodic | 為了協助管理資產庫存清單，此規則會檢查安全群組是否連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或彈性網路介面。如果安全群組未連接到這些資源類型，可能未使用且不再需要這些安全群組。 |
| 4.3. 驗證 - 庫存清單 | 應該提供所有相關系統及其 GMP 功能的最新清單 (庫存清單)。對於重要系統，應提供最新的系統描述，詳細說明實體和邏輯排列、與其他系統或程序之間的資料流程和介面、任何硬體和軟體先決條件以及安全措施。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.3. 驗證 - 庫存清單 | 應該提供所有相關系統及其 GMP 功能的最新清單 (庫存清單)。對於重要系統，應提供最新的系統描述，詳細說明實體和邏輯排列、與其他系統或程序之間的資料流程和介面、任何硬體和軟體先決條件以及安全措施。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| 4.3. 驗證 - 庫存清單 | 應該提供所有相關系統及其 GMP 功能的最新清單 (庫存清單)。對於重要系統，應提供最新的系統描述，詳細說明實體和邏輯排列、與其他系統或程序之間的資料流程和介面、任何硬體和軟體先決條件以及安全措施。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 4.8. 驗證 - 資料傳輸 | 如果將資料傳輸至另一種資料格式或系統，驗證應包括檢查資料的價值和/或意義在此遷移過程中未改變。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 5. 資料 | 以電子方式與其他系統交換資料的電腦化系統應包含適當的內建檢查，用來正確且安全地輸入和處理資料，以便將風險降至最低。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 7.1. 資料儲存 - 損壞保護 | 應透過物理和電子方式保護資料免遭損壞。應檢查儲存資料的可存取性、可讀性及準確性。應確保在整個保留期間的資料存取。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 7.2. 資料儲存 - 備份 | 應定期備份所有相關資料。應在驗證過程中檢查並定期監控備份資料的完整性和準確性以及還原資料的能力。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9. 稽核記錄 | 應根據風險評估，考慮在系統中建置所有 GMP 相關變更和刪除的記錄 (系統產生的「稽核記錄」)。應記載變更或刪除 GMP 相關資料的原因。稽核記錄必須可供使用、可轉換為一般可理解的形式，並需要定期檢閱。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| 10. 變更與組態管理 | 電腦化系統的任何變更 (包括系統組態) 只能根據定義的程序以受控方式進行。 | elb-deletion-prote ction-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| 10. 變更與組態管理 | 電腦化系統的任何變更 (包括系統組態) 只能根據定義的程序以受控方式進行。 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10. 變更與組態管理 | 電腦化系統的任何變更 (包括系統組態) 只能根據定義的程序以受控方式進行。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| 11. 定期評估 | 應定期評估電腦化系統，以確認其保持有效狀態並符合 GMP。此類評估應適當地包括目前的功能範圍、偏差記錄、事件、問題、升級歷程記錄、效能、可靠性、安全及驗證狀態報告。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | ecs-containers-non privileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | rds-instance-iam-authentication-enabled | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體上啟用 AWS 身分和存取管理 (IAM) 身份驗證，以控制對系統和資產的存取。這會強制使用 Secure Sockets Layer (SSL) 來加密往返資料庫的網路流量。您不需要將使用者憑證放在資料庫，因為身分驗證是由外部管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 12.1. 安全 - 授權人員 | 應採取實體和/或邏輯控制，限制只有授權人員才能存取電腦化系統。防止未經授權進入系統的適當方法可能包括使用金鑰、通行卡、含有密碼的個人代碼、生物特徵辨識、限制存取電腦設備及資料儲存區。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.3. 安全 - 授權稽核記錄 | 應記錄存取授權的建立、變更及取消。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12.4. 安全 - 稽核記錄 | 用於資料和文件的管理系統應該設計為記錄輸入、變更、確認或刪除資料 (包括日期和時間) 的操作員身分。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 13. 事件管理 | 應報告及評估所有事件，而不僅僅是系統故障和資料錯誤。應識別嚴重事件的根本原因，並構成修正和預防動作的基礎。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 13. 事件管理 | 應報告及評估所有事件，而不僅僅是系統故障和資料錯誤。應識別嚴重事件的根本原因，並構成修正和預防動作的基礎。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時(例如手動或替代系統)能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時(例如手動或替代系統)能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時(例如手動或替代系統)能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | lambda-vpc-multi-az-check | 如果您的 AWS Lambda 函數設定為連線到帳戶中的虛擬私有雲 (VPC)，請在至少兩個不同的可用區域中部署 AWS Lambda 函數，以確保在單一區域中發生服務中斷時，它是您的函數可用來處理事件。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | opensearch-data-node-fault-tolerance | Amazon OpenSearch 服務 (服OpenSearch 務) 至少需要三個資料節點才能達到高可用性和容錯能力。部署具有至少三個資料節點的 OpenSearch Service 網域可確保節點失敗時的叢集作業。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時(例如手動或替代系統)能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時(例如手動或替代系統)能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 16. 業務持續性 | 至於支援關鍵程序的電腦化系統可供使用，應制定條文，以確保在系統發生故障時 (例如手動或替代系統) 能夠持續支援這些程序。使用替代安排所需的時間應以風險為基礎，並適用於特定系統及其所支援的業務程序。這些安排應經適當分記載和測試。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 17. 封存 | 資料可以進行封存。應檢查此資料的可存取性、可讀性及完整性。如果要對系統進行相關更改（例如計算機設備或程序），則應確保和測試檢索數據的能力。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

## 範本

該模板可在以下網站獲得 GitHub：GxP 歐盟附件 11 的操作最佳實踐。

# HIPAA 安全的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了 Health 保險可攜性與責任法案 (HIPAA) 與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 HIPAA 控制項相關。一個 HIPAA 控制項可與多項組態規則相關聯。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

本一致性套件由 AWS 安全保證服務 LLC (AWS SAS) 驗證，該公司是由支付卡產業合格安全評估機構 (QSA)、HITRUST 認證共同安全框架從業人員 (CCSFP) 以及經過認證的合規專業人員組成的團隊，可為各種產業框架提供指導和評估。 AWS SAS 專業人員設計了此一符合性套件，使客戶能夠與 HIPAA 的子集保持一致。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(A) | (A) 風險分析 (必要)。對受保護實體持有之受保護電子健康資訊的機密性、完整性和可用性，執行準確而全面的潛在風險和漏洞評估。 | annual-risk-assessment-performed (處理程序檢查) | 對貴組織執行年度風險評估。風險評估可協助確定已識別風險和/或漏洞影響組織的可能性及影響內容。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | | (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) 風險管理 (必要)。實作足以將風險和漏洞降低到合理和適當水平的安全措施，以符合第 164.306(a) 條的規定。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) 標準：勞工安全。實作政策和程序，以確保所有工作人員都能適當獲取本節 (a)(4) 條所述之受保護電子健康資訊，並防止依本節 (a)(4) 條規定無權存取受保護電子健康資訊的工作人員取得此類相關資訊。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 164.308(a)(3)(ii)(A) | (A) 授權和/或監督 (可定址)。實作授權和/或監督工作人員的程序，使其得以使用受保護電子健康資訊，或使用位在可能被存取位置的受保護電子健康資訊。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) 工作人員清除程序 (可定址)。實作可判定工作人員存取受保護電子健康資訊適當與否的程序。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 164.308(a)(3)(ii)(C) | (C) 終止程序 (可定址)。在僱用工作人員僱用終止時，或按本節第 (a)(3)(ii)(B) 條明定規範所要求，實作終止存取受保護電子健康資訊的程序。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 164.308(a)(4)(i) | (4)(i) 標準：資訊存取管理。實作政策及程序，以授權存取符合本編 E 分編適用規定的受保護電子健康資訊。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) 隔離醫療保健資訊交換所功能 (必要)。如果醫療保健資訊交換所屬於較大型的組織，則資訊交換所必須實作政策和程序，以保護資訊交換所的受保護電子健康資訊免於大型組織的未經授權存取。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) 存取授權 (可定址)。實作政策和程序以授予受保護電子健康資訊的存取權限，例如，透過工作站、交易、程式、程序的存取權或其他機制。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權(可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 164.308(a)(4)(ii)(C) | (C) 建立和修改存取權 (可定址)。根據實體的存取授權政策，實作政策與程序，以建立、記錄、檢閱和修改使用者的工作站、交易、程式或程序存取權。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(A) | (A) 安全提醒 (可定址)。定期的安全性更新。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 164.308(a)(5)(ii)(A) | (A) 安全提醒 (可定址)。定期的安全性更新。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(A) | (A) 安全提醒 (可定址)。定期的安全性更新。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 164.308(a)(5)(ii)(A) | (A) 安全提醒 (可定址)。定期的安全性更新。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(B) | (B) 防範惡意軟體 (可定址)。防範、偵測和報告惡意軟體的程序。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 164.308(a)(5)(ii)(B) | (B) 防範惡意軟體 (可定址)。防範、偵測和報告惡意軟體的程序。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(B) | (B) 防範惡意軟體 (可定址)。防範、偵測和報告惡意軟體的程序。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 164.308(a)(5)(ii)(C) | (C) 登入監控 (可定址)。監控登錄嘗試和報告差異的程序。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 164.308(a)(5)(ii)(C) | (C) 登入監控 (可定址)。監控登錄嘗試和報告差異的程序。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(C) | (C) 登入監控 (可定址)。監控登錄嘗試和報告差異的程序。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(D) | (D) 密碼管理 (可定址)。建立、變更及保護密碼的程序。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(6)(i) | (6)(i) 標準：安全事件程序。實作政策和程序以處理安全事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 164.308(a)(6)(ii) | (ii) 實作規範：回應和報告 (必要)。識別並回應可疑或已知的安全事件；在可行的範圍內減少受保護實體已知安全事件的有害影響；以及記錄安全事件及其結果。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 164.308(a)(7)(i) | (7)(i) 標準：緊急應變計畫。建立 (並視需要實作) 政策和程序，以因應對包含受保護電子健康資訊之系統造成損害的緊急事件或其他事件 (例如火災、人為破壞、系統故障和自然災害)。 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) 資料備份計畫 (必要)。建立並實作程序，以建立和維護可擷取的受保護電子健康資訊的精確副本。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) 災難復原計畫 (必要)。建立 (並視需要實作) 程序以還原遺失的資料。 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| 164.308(a)(7)(ii)(C) | (C) 緊急模式操作計畫 (必要)。建立 (並視需要實作) 程序以延續關鍵業務流程，以便在緊急模式中操作時，為受保護的電子健康資訊提供安全防護。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 164.308(a)(7)(ii)(C) | (C) 緊急模式操作計畫 (必要)。建立 (並視需要實作) 程序以延續關鍵業務流程，以便在緊急模式中操作時，為受保護的電子健康資訊提供安全防護。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(C) | (C) 緊急模式操作計畫 (必要)。建立 (並視需要實作) 程序以延續關鍵業務流程，以便在緊急模式中操作時，為受保護的電子健康資訊提供安全防護。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 164.308(a)(7)(ii)(C) | (C) 緊急模式操作計畫 (必要)。建立 (並視需要實作) 程序以延續關鍵業務流程，以便在緊急模式中操作時，為受保護的電子健康資訊提供安全防護。 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(C) | (C) 緊急模式操作計畫 (必要)。建立 (並視需要實作) 程序以延續關鍵業務流程，以便在緊急模式中操作時，為受保護的電子健康資訊提供安全防護。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(C) | (C) 緊急模式操作計畫 (必要)。建立 (並視需要實作) 程序以延續關鍵業務流程，以便在緊急模式中操作時，為受保護的電子健康資訊提供安全防護。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 164.308(a)(8) | (8) 標準：評估。一開始按本規則實作的標準為準，定期執行技術和非技術性評估，然後根據影響受保護電子健康資訊安全性的環境或操作變化，確定實體安全政策和程序達到本分編要求的程度。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.308(a)(8) | (8) 標準：評估。一開始按本規則實作的標準為準，定期執行技術和非技術性評估，然後根據影響受保護電子健康資訊安全性的環境或操作變化，確定實體安全政策和程序達到本分編要求的程度。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 164.312(a)(1) | (a)(1) 標準：存取控制。實作技術政策和程序，讓維護受保護電子健康資訊的電子資訊系統只允許將存取權授予依 ¤ 164.308(a)(4) 規定可被授予存取權限的人士或軟體程式。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(i) | (2) 實作規範：(i) 唯一的使用者識別 (必要)。指派唯一的名稱和/或號碼，以供識別與追蹤使用者身分。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays （Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) 緊急存取程序 (必要)。建立 (並視需要實作) 程序，以在緊急情況下獲取必要的受保護電子健康資訊。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(a)(2)(iv) | (iv) 加密和解密 (可定址)。實作加密和解密受保護電子健康資訊的機制。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。警示範例包括：建立新物件、移除物件、還原物件、遺失和複製物件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(b) | (b) 標準：稽核控制項。實作硬體、軟體和/或程序機制，以記錄和檢查包含或使用受保護電子健康資訊之資訊系統中的活動。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 164.312(c)(1) | (c)(1) 標準：完整性。實作政策和程序，以保護受保護電子健康資訊免於不當更改或破壞。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(c)(1) | (c)(1) 標準：完整性。實作政策和程序，以保護受保護電子健康資訊免於不當更改或破壞。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 164.312(c)(1) | (c)(1) 標準：完整性。實作政策和程序，以保護受保護電子健康資訊免於不當更改或破壞。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(c)(1) | (c)(1) 標準：完整性。實作政策和程序，以保護受保護電子健康資訊免於不當更改或破壞。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 164.312(c)(1) | (c)(1) 標準：完整性。實作政策和程序，以保護受保護電子健康資訊免於不當更改或破壞。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(c)(2) | (2) 實作規範：驗證受保護電子健康資訊的機制 (可定址)。實作電子機制，以證實受保護電子健康資訊未經非授權方式更改或破壞。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 164.312(c)(2) | (2) 實作規範：驗證受保護電子健康資訊的機制 (可定址)。實作電子機制，以證實受保護電子健康資訊未經非授權方式更改或破壞。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(c)(2) | (2) 實作規範：驗證受保護電子健康資訊的機制 (可定址)。實作電子機制，以證實受保護電子健康資訊未經非授權方式更改或破壞。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 164.312(c)(2) | (2) 實作規範：驗證受保護電子健康資訊的機制 (可定址)。實作電子機制，以證實受保護電子健康資訊未經非授權方式更改或破壞。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(c)(2) | (2) 實作規範：驗證受保護電子健康資訊的機制 (可定址)。實作電子機制，以證實受保護電子健康資訊未經非授權方式更改或破壞。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(d) | (d) 標準：個人或實體驗證。實作程序以驗證欲存取受保護電子健康資訊的個人或實體，是否確為個人或實體。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(d) | (d) 標準：個人或實體驗證。實作程序以驗證欲存取受保護電子健康資訊的個人或實體，是否確為個人或實體。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 164.312(d) | (d) 標準：個人或實體驗證。實作程序以驗證欲存取受保護電子健康資訊的個人或實體，是否確為個人或實體。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(d) | (d) 標準：個人或實體驗證。實作程序以驗證欲存取受保護電子健康資訊的個人或實體，是否確為個人或實體。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 164.312(d) | (d) 標準：個人或實體驗證。實作程序以驗證欲存取受保護電子健康資訊的個人或實體，是否確為個人或實體。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可防止儲存貯體層級的公開存取，協助保護敏感資料免受未經授權的遠端使用者存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 164.312(e)(1) | (e)(1) 標準：傳輸安全性。實作技術安全措施，以防止未經授權存取正透過電子通信網路傳輸的受保護電子健康資訊。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) 完整性控制項 (可定址)。實作安全措施，以確保以電子方式傳輸的受保護電子健康資訊不會在處置前，在未經偵測的情況下進行不當修改。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.312(e)(2)(ii) | (ii) 加密 (可定址)。只要認為適當，即實作加密受保護電子健康資訊的機制。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) 標準：團體醫療保險計畫的要求。除非僅向計畫主辦單位揭露的受保護電子健康資訊根據 ¤ 164.504(f)(1)(ii) 或 (iii) 或依 ¤ 164.508 授權而公開，否則團體醫療保險計畫必須確保其計劃文件規定，計畫主辦單位會以合理且適當的方式保護計畫主辦單位代團體醫療保險計畫所建立、接收、維護或傳送的受保護電子健康資訊。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性；(ii) 確保以合理且適當的安全措施支援 ¤ 164.504(f)(2)(iii) 要求之適當分離；(iii) 確保收到此資訊的所有客服人員 (包括外包人員在內)，皆同意實作合理且適當的安全措施以保護此資訊；以及 (iv) 向團體醫療保險計畫報告任何已察覺到的安全事件。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 164.314(b)(2)(i) | (2) 實作規範 (必要)。團體醫療保險計畫的計畫文件必須加以修改，納入對計畫主辦單位的要求：(i) 實作行政、實際和技術保護措施，以合理且適當的方式保護其代團體醫療保險計畫所建立、接收、維護或傳輸之受保護電子健康資訊的機密性、完整性和可用性； | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

## 範本

範本可在下列網站取得 GitHub：HIPAA 安全性的營運最佳作法。

# IRS 1075 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了 IRS 1075 與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 IRS 1075 控制項相關。一個 IRS 1075 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 d. 傳輸中的資料加密 | 在雲端環境中傳輸的 FTI 必須進行加密。用於加密 FTI 的所有機制都必須通過 FIPS 140 認證，並利用最新的 FIPS 140 合規模組來運作。必須在 SLA 中包含此要求。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.3.1 雲端運算 d. 傳輸中的資料加密 | 在雲端環境中傳輸的 FTI 必須進行加密。用於加密 FTI 的所有機制都必須通過 FIPS 140 認證，並利用最新的 FIPS 140 合規模組來運作。必須在 SLA 中包含此要求。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.3.1 雲端運算 d. 傳輸中的資料加密 | 在雲端環境中傳輸的 FTI 必須進行加密。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 用於加密 FTI 的所有機制都必須通過 FIPS 140 認證，並利用最新的 FIPS 140 合規模組來運作。必須在 SLA 中包含此要求。 | | 設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.3.1 雲端運算 d. 傳輸中的資料加密 | 在雲端環境中傳輸的 FTI 必須進行加密。用於加密 FTI 的所有機制都必須通過 FIPS 140 認證，並利用最新的 FIPS 140 合規模組來運作。必須在 SLA 中包含此要求。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 3.3.1 雲端運算 d. 傳輸中的資料加密 | 在雲端環境中傳輸的 FTI 必須進行加密。用於加密 FTI 的所有機制都必須通過 FIPS 140 認證，並利用最新的 FIPS 140 合規模組來運作。必須在 SLA 中包含此要求。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 d. 傳輸中的資料加密 | 在雲端環境中傳輸的 FTI 必須進行加密。用於加密 FTI 的所有機制都必須通過 FIPS 140 認證，並利用最新的 FIPS 140 合規模組來運作。必須在 SLA 中包含此要求。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.3.1 雲端運算 d. 傳輸中的資料加密 | 在雲端環境中傳輸的 FTI 必須進行加密。用於加密 FTI 的所有機制都必須通過 FIPS 140 認證，並利用最新的 FIPS 140 合規模組來運作。必須在 SLA 中包含此要求。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 3.3.1 雲端運算 e. 靜態資料加密 | 靜態資料加密：雲端中的靜態 FTI 必須使用最新的 FIPS 140 認證加密機制進行加密。必須在 SLA 中包含此要求。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.3.1 雲端運算 k. 多重要素驗證 | 當機構從網際網路提供其雲端解決方案時 (即從機構信任的網路外部存取雲端解決方案)，必須實作足夠的多重要素驗證。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 k. 多重要素驗證 | 當機構從網際網路提供其雲端解決方案時 (即從機構信任的網路外部存取雲端解決方案)，必須實作足夠的多重要素驗證。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 3.3.1 雲端運算 k. 多重要素驗證 | 當機構從網際網路提供其雲端解決方案時 (即從機構信任的網路外部存取雲端解決方案)，必須實作足夠的多重要素驗證。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 雲端運算 k. 多重要素驗證 | 當機構從網際網路提供其雲端解決方案時 (即從機構信任的網路外部存取雲端解決方案)，必須實作足夠的多重要素驗證。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 3.3.1 雲端運算 i. 風險評估： | 機構必須對用於接收、處理、儲存、存取、保護和/或傳輸 FTI 的所有資訊系統，每年進行適當的安全和隱私評估。 | annual-risk-assessment-performed (程序檢查) | 對貴組織執行年度風險評定。風險評估可協助確定已識別風險和/或漏洞影響組織的可能性及影響內容。 |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | netfw-policy-rule-group-associated | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包與流量流程，並定義預設流量處理。 |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | waf-regional-rule-not-empty | 確保 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 3.3.6 網路邊界和基礎設施 | 機構必須在整個系統架構中實作邊界防護裝置 (包括路由器、防火牆、交換器和入侵偵測系統)，以便保護 FTI 和 FTI 系統。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (f) | 根據機構帳戶管理程序的先決條件，建立、啟用、修改、停用和移除帳戶； | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-2 帳戶管理 (f) | 根據機構帳戶管理程序的先決條件，建立、啟用、修改、停用和移除帳戶； | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (f) | 根據機構帳戶管理程序的先決條件，建立、啟用、修改、停用和移除帳戶； | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-2 帳戶管理 (f) | 根據機構帳戶管理程序的先決條件，建立、啟用、修改、停用和移除帳戶； | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| AC-2 帳戶管理 (f) | 根據機構帳戶管理程序的先決條件，建立、啟用、修改、停用和移除帳戶； | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (g) | 監控帳戶的使用 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | secretsmanager-secret-periodic-rotation | 此規則可確保「AWS Secrets Manager」密碼已啟用定期輪換。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。預設值為 90 天。 |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC-2 帳戶管理 (j) | 檢閱帳戶是否符合帳戶管理要求 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| (CE-1) 自動化系統帳戶管理 | 支援使用自動化機制管理系統帳戶。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| (CE-1) 自動化系統帳戶管理 | 支援使用自動化機制管理系統帳戶。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| (CE-1) 自動化系統帳戶管理 | 支援使用自動化機制管理系統帳戶。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| (CE-3)：停用帳戶 | 當帳戶發生下列情況時，在 120 天內停用帳戶：a. 已過期；b. 不再與使用者或個人相關聯；c. 違反組織政策；或 d. 未使用達 120 天 (若為非特殊權限帳戶) 或 60 天 (若為特殊權限帳戶) | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| (CE-12) 監控帳戶的非典型使用情況 | 監控系統帳戶中是否有機構定義的非典型使用情況；以及向機構定義的人員或角色報告系統帳戶的非典型使用情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC-6 最低權限 | 運用最低權限原則，僅授予使用者 (或代表使用者處理的程序) 完成指派組織任務所需的存取權。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| AC-17：遠端存取 | 為允許的每種遠端存取類型，建立和記載使用限制、組態/連線要求和實作指引；以及授權系統的每種遠端存取類型，再允許此連線。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| AT-1：意識和培訓 | 為系統使用者 (包括管理員、高階主管和承包商) 提供安全和隱私素養培訓 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計畫可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |
| AU-2：稽核事件 | 識別系統能夠記錄以支援稽核功能的事件類型 | audit-log-policy-exists (程序檢查) | 建立並維護稽核日誌管理原則，以定義組織的日誌記錄需求。這包括但不限於檢閱和保留稽核日誌。 |
| AU-16：跨組織稽核日誌記錄 | 跨組織邊界傳輸機稽核資訊時，運用機構定義的方法在外部組織之間協調機構定義的稽核資訊。 | audit-log-policy-exists (程序檢查) | 建立並維護稽核日誌管理原則，以定義組織的日誌記錄需求。這包括但不限於檢閱和保留稽核日誌。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CA-7：持續監控 | 根據組織層級的持續監控策略，制定系統層級的持續監控策略，並實作持續監控：建立要加以監控的機構定義指標；根據持續監控策略進行持續控制評估；根據持續監控策略對系統和組織定義的指標進行持續監控；將控制評估和監控所產生的資訊相互關聯並進行分析；採取回應行動，以解決控制評估和監控資訊的分析結果；並至少每年向機構定義的人員報告系統的安全和隱私狀態。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CP-9：系統備份 | a. 每週對系統中包含的使用者層級資訊進行備份，包括安全相關文件；b. 每週對系統中包含的系統層級資訊進行備份；c. 每週對系統文件進行備份，包括安全和隱私相關文件；以及 d. 保護備份資訊的機密性、完整性和可用性。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| IA-2：識別與驗證 (組織使用者) (CE-1) 特殊權限帳戶的多重要素驗證 | 實作多重要素驗證以存取特殊權限帳戶 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA-2：識別與驗證 (組織使用者) (CE-1) 特殊權限帳戶的多重要素驗證 | 實作多重要素驗證以存取特殊權限帳戶 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-2：識別與驗證 (組織使用者) (CE-2) 非特殊權限帳戶的多重要素驗證 | 實作多重要素驗證以存取非特殊權限帳戶。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| IA-5：驗證器管理：(CE-1) 密碼型驗證：若要進行密碼型驗證 | 強制執行以下組成和複雜性規則：1. 強制執行十四 (14) 個字元的密碼長度下限。2. 強制執行最低密碼複雜性，以包含數字、大寫字母、小寫字母和特殊字元的組合。3. 選擇要使用的新密碼時，強制至少變更一 (1) 個字元。4. 僅儲存和傳輸以密碼編譯方式保護的密碼。5. 強制執行密碼存留期限制：i. 最少一 (1) 天，最多 90 天。ii. 服務帳戶密碼應在 366 天 (含) 內到期。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PM-5：系統清查 | 持續制定和更新組織系統的清查。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| PM-5：系統清查 | 持續制定和更新組織系統的清查。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PM-5：系統清查 | 持續制定和更新組織系統的清查。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| PM-5：系統清查 | 持續制定和更新組織系統的清查。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| RA-5：漏洞監控和掃描 | 在將新的資訊系統置於機構網路之前，每三十 (30) 天監控並掃描系統及託管應用程式中的漏洞以確認修復動作，並在找到及報告可能影響系統/應用程式的新漏洞時進行監控和掃描 | vuln-scans-performed (程序檢查) | 確保根據您的合規要求執行漏洞掃描。貴組織應定義掃描的頻率、使用的工具以及結果的使用方式。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SA-10：開發人員組態管理 (e.) | 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SA-10：開發人員組態管理 (e.) | 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SA-10：開發人員組態管理 (e.) | 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SA-10：開發人員組態管理 (a) (c.) | 在系統、元件或服務設計、開發、實作、操作期間執行組態管理；只對系統、元件或服務實作組織核准的變更； | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SC-4：共用系統資源中的資訊 | 防止未經授權和意外透過共用的系統資源傳輸資訊 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 | 在系統的外部邊界和系統內的關鍵內部邊界監控和控制通訊；實作與內部組織網路分開之可公開存取的系統元件子網路；以及只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構安排的邊界防護裝置。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7：邊界防護 (CE-9) 限制具威脅性的傳出通訊流量 | 偵測對外部系統構成威脅的傳出通訊流量並加以拒絕；以及稽核與遭拒通訊相關的內部使用者身分。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 (CE-9) 限制具威脅性的傳出通訊流量 | 偵測對外部系統構成威脅的傳出通訊流量並加以拒絕；以及稽核與遭拒通訊相關的內部使用者身分。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC-7：邊界防護 (CE-9) 限制具威脅性的傳出通訊流量 | 偵測對外部系統構成威脅的傳出通訊流量並加以拒絕；以及稽核與遭拒通訊相關的內部使用者身分。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| SC-7：邊界防護 (IRS 定義) | 機構應在信任邊界實作和管理邊界防護 (通常使用防火牆)。每個信任邊界都應受到監控，並應控制跨每個邊界進行的通訊。 | netfw-policy-rule-group-associated | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包與流量流程，並定義預設流量處理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-7：邊界防護 (IRS 定義) | 機構應在信任邊界實作和管理邊界防護 (通常使用防火牆)。每個信任邊界都應受到監控，並應控制跨每個邊界進行的通訊。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |
| SC-8：傳輸機密性與完整性 (CE-1) 密碼編譯保護 | 在傳輸過程中實作密碼編譯機制，以防止未經授權洩漏資訊，並偵測資訊變更。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8：傳輸機密性與完整性 (CE-1) 密碼編譯保護 | 在傳輸過程中實作密碼編譯機制，以防止未經授權洩漏資訊，並偵測資訊變更。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-8：傳輸機密性與完整性 (CE-1) 密碼編譯保護 | 在傳輸過程中實作密碼編譯機制，以防止未經授權洩漏資訊，並偵測資訊變更。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8：傳輸機密性與完整性 (CE-1) 密碼編譯保護 | 在傳輸過程中實作密碼編譯機制，以防止未經授權洩漏資訊，並偵測資訊變更。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| SC-8：傳輸機密性與完整性 (CE-1) 密碼編譯保護 | 在傳輸過程中實作密碼編譯機制，以防止未經授權洩漏資訊，並偵測資訊變更。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-8：傳輸機密性與完整性 (CE-1) 密碼編譯保護 | 在傳輸過程中實作密碼編譯機制，以防止未經授權洩漏資訊，並偵測資訊變更。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8：傳輸機密性與完整性 (CE-1) 密碼編譯保護 | 在傳輸過程中實作密碼編譯機制，以防止未經授權洩漏資訊，並偵測資訊變更。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-12：密碼編譯金鑰建立與管理 | 當機構在系統中採用密碼編譯時，必須根據下列金鑰管理要求建立和管理密碼編譯金鑰：NIST SP 800-57，關於金鑰產生、分佈、儲存、存取和銷毀的金鑰管理建議。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-12：密碼編譯金鑰建立與管理 | 當機構在系統中採用密碼編譯時，必須根據下列金鑰管理要求建立和管理密碼編譯金鑰：NIST SP 800-57，關於金鑰產生、分佈、儲存、存取和銷毀的金鑰管理建議。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC-13：密碼編譯保護 | 實作以下每個指定密碼編譯用途所需的密碼編譯類型：最新的 FIPS-140 驗證加密機制；NIST 800-52；Transport Layer Security (TLS) 實作的選擇、設定和使用指南；傳輸中加密 (承載加密)。禁止將 SHA-1 用於數位簽章。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-23：工作階段真確性 | 保護通訊工作階段的真確性。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC-28：保護靜態資訊 (CE-1) 密碼編譯保護 | 實作密碼編譯機制，以防止未經授權洩漏和修改終端使用者運算系統 (例如桌上型電腦、筆記型電腦、行動裝置、可攜式和抽取式存放裝置) 上非揮發性儲存中的靜態 FTI。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-2：瑕疵修復 (IRS 定義) | 該機構應確保在每天啟動並連接到機構網絡時，檢查工作站（如政策中所定義，包括使用 GFE 工作站的遠程連接），以確保已應用最新的代理商批准的修補程序，並根據需要應用任何缺席或新的補丁程序，或者檢查不得超過每 24 小時（週末，假日等） | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SI-2：瑕疵修復 (IRS 定義) | 該機構應確保在每天啟動並連接到機構網絡時，檢查工作站（如政策中所定義，包括使用 GFE 工作站的遠程連接），以確保已應用最新的代理商批准的修補程序，並根據需要應用任何缺席或新的補丁程序，或者檢查不得超過每 24 小時（週末，假日等） | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-2：瑕疵修復 (IRS 定義) | 該機構應確保在每天啟動並連接到機構網絡時，檢查工作站（如政策中所定義，包括使用 GFE 工作站的遠程連接），以確保已應用最新的代理商批准的修補程序，並根據需要應用任何缺席或新的補丁程序，或者檢查不得超過每 24 小時（週末，假日等） | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SI-2：瑕疵修復 (IRS 定義) | 該機構應確保在每天啟動並連接到機構網絡時，檢查工作站（如政策中所定義，包括使用 GFE 工作站的遠程連接），以確保已應用最新的代理商批准的修補程序，並根據需要應用任何缺席或新的補丁程序，或者檢查不得超過每 24 小時（週末，假日等） | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-2：瑕疵修復 (IRS 定義) | 該機構應確保在每天啟動並連接到機構網絡時，檢查工作站（如政策中所定義，包括使用 GFE 工作站的遠程連接），以確保已應用最新的代理商批准的修補程序，並根據需要應用任何缺席或新的補丁程序，或者檢查不得超過每 24 小時（週末，假日等） | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| SI-2：瑕疵修復 (IRS 定義) | 該機構應確保在每天啟動並連接到機構網絡時，檢查工作站（如政策中所定義，包括使用 GFE 工作站的遠程連接），以確保已應用最新的代理商批准的修補程序，並根據需要應用任何缺席或新的補丁程序，或者檢查不得超過每 24 小時（週末，假日等） | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 透過 [指派: 組織定義的技術和方法] 識別未經授權的資訊系統使用；c. 部署監控裝置：1. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 2. 在系統內的特定位置，追蹤組織感興趣的特定交易類型；d. 保護從入侵監控工具取得的資訊，以防止未經授權的存取、修改和刪除； | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 透過 [指派: 組織定義的技術和方法] 識別未經授權的資訊系統使用；c. 部署監控裝置：1. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 2. 在系統內的特定位置，追蹤組織感興趣的特定交易類型；d. 保護從入侵監控工具取得的資訊，以防止未經授權的存取、修改和刪除； | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 透過 [指派: 組織定義的技術和方法] 識別未經授權的資訊系統使用；c. 部署監控裝置：1. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 2. 在系統內的特定位置，追蹤組織感興趣的特定交易類型；d. 保護從入侵監控工具取得的資訊，以防止未經授權的存取、修改和刪除； | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 透過 [指派: 組織定義的技術和方法] 識別未經授權的資訊系統使用；c. 部署監控裝置：1. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 2. 在系統內的特定位置，追蹤組織感興趣的特定交易類型；d. 保護從入侵監控工具取得的資訊，以防止未經授權的存取、修改和刪除； | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 透過 [指派: 組織定義的技術和方法] 識別未經授權的資訊系統使用；c. 部署監控裝置：1. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 2. 在系統內的特定位置，追蹤組織感興趣的特定交易類型；d. 保護從入侵監控工具取得的資訊，以防止未經授權的存取、修改和刪除； | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-4：系統監控 (IRS 定義) | 所有網際網路存取點/入口網站都應擷取傳入和傳出流量標頭資訊並保留至少一年，但不包括已核准的網際網路「匿名」連線，因為這些連線可能是由機構 CISO 核准。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| SI-7：軟體、韌體和資訊完整性 | 使用完整性驗證工具來偵測下列軟體、韌體和資訊的未經授權變更：系統核心、驅動程式、韌體 (例如 BIOS、UEFI)、軟體 (例如作業系統、應用程式、中介軟體) 和安全性屬性。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-7：軟體、韌體和資訊完整性 | 使用完整性驗證工具來偵測下列軟體、韌體和資訊的未經授權變更：系統核心、驅動程式、韌體 (例如 BIOS、UEFI)、軟體 (例如作業系統、應用程式、中介軟體) 和安全性屬性。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SI-7：軟體、韌體和資訊完整性 | 使用完整性驗證工具來偵測下列軟體、韌體和資訊的未經授權變更：系統核心、驅動程式、韌體 (例如 BIOS、UEFI)、軟體 (例如作業系統、應用程式、中介軟體) 和安全性屬性。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | dynamodb-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 資源是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | ebs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | efs-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | rds-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | s3-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| SI-12：資訊管理與保留 | 根據適用的法律、行政命令、指令、法規、政策、標準、準則和營運要求，管理和保留系統內的資訊以及系統輸出的資訊。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

### 範本

該模板可用於 GitHub：國稅局 1075 的操作最佳實踐。

## K-ISMS 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了韓國-信息安全管理系統（ISMS）和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則都適用於特定 AWS 資源，並與一或多個 Korea – ISMS 控制項相關。一個 Korea – ISMS 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.2.1 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 1.2.1 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| 2.1.3 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 2.1.3 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| 2.3.3 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 2.3.3 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.1 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 2.5.1 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.1 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 2.5.1 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.1 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 2.5.1 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 2.5.1 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.1 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 2.5.1 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 2.5.1 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 2.5.1 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 2.5.1 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.1 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.5.3 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 2.5.3 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.3 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 2.5.4 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5.5 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 2.5.5 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 2.5.5 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 2.6 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 2.6 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 2.6 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 2.6 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 2.6 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 2.6 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 2.6 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 2.6 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 2.6 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 2.6 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 2.6 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 2.6 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 2.6 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 2.6 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6.6 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 2.6.6 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 2.6.6 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 2.6.6 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6.6 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 2.6.6 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6.6 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 2.6.6 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 2.6.6 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.6.6 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 2.6.6 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 2.6.6 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 2.6.7 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.7 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 2.7 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.7 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.7 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.7 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.7 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 2.7 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 2.7 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.7 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 2.7 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.7 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.7 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 2.7 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.7 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.7 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.7 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.7 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 2.7 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.7 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 2.7 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.7 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 2.7 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.7 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於發佈的訊息中可能存在靜態的敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.7 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 2.7 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.7.1 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.7.1 | elb-predefined-security-policy-ssl-check | 為協助保護傳輸中的資料，請確定您的 Classic Elastic Load Balancing SSL 接聽程式使用預先定義的安全政策。Elastic Load Balancing 提供預先定義的 SSL 溝通組態，其在用戶端和負載平衡器之間建立連線時用於 SSL 溝通。SSL 溝通組態能與廣泛的用戶端相容，並使用高強度的密碼編譯演算法。此規則需要您設定預先定義的 SSL 接聽程式安全政策。預設的安全性原則為：EL SecurityPolicy B 實際值應反映貴組織的政策。 |
| 2.7.2 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 2.7.2 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.8.5 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 2.8.5 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 2.8.6 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 2.8.6 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌，AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.1 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 2.9.1 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 2.9.1 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.1 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 2.9.2 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體不回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.2 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 2.9.2 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 2.9.2 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並在 1 分鐘內顯示執行個體的監控圖形。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.2 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| 2.9.2 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| 2.9.3 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力需求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.3 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 2.9.3 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2.9.3 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.3 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2.9.3 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 2.9.3 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| 2.9.3 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.3 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| 2.9.3 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.3 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 2.9.3 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| 2.9.3 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.3 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 2.9.3 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 2.9.3 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.3 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2.9.4 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 2.9.4 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 2.9.4 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 2.9.4 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.4 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 2.9.4 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 2.9.4 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.4 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 2.9.4 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 2.9.4 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.9.4 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 2.10.3 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| 2.10.3 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.10.3 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 2.10.3 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 2.10.3 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.10.5 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.10.5 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.10.5 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.10.5 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.10.5 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.10.5 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.10.5 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.10.5 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.10.8 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 2.10.8 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 2.11.2 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.11.3 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、 insufficientDataAction 必要 (Config 預設值：True)、okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 2.11.3 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並在 1 分鐘內顯示執行個體的監控圖形。 |
| 2.11.3 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 2.11.3 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.11.3 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| 2.11.3 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.12 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| 2.12 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 2.12 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.12 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2.12 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2.12 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.12 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理遺失一或多個執行個體的能力。 |
| 2.12 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 2.12 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| 2.12 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.12 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 2.12 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 2.12 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.12 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 2.12 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 2.12 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.12 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2.12 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

### 範本

該模板可用於 GitHub：K-ISMS 的操作最佳實踐。

## 負載平衡的操作最佳實務

此一致性套件包含以內部負載平衡為基礎的 AWS Config 規則。 AWS如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

樣板位於 GitHub：負載平衡的作業最佳作法。

## 日誌的操作最佳實務

此一致性套件包含以內部記錄為基礎的 AWS Config 規則。 AWS如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本位於 GitHub：記錄的操作最佳作法。

## 管理與控管服務的操作最佳實務

此符合性套件包含以管理與治理服務為基礎的 AWS Config 規則。如需詳細資訊，請參閱上的管理和控管 AWS。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：管理與治理服務的最佳營運實務。

## MAS Notice 655 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了新加坡金融管理局（MAS）公告 655-網絡衛生和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則適用於特定 AWS 資源，並與一個或多個 MAS 通知 655-網絡衛生控制相關。一個 MAS Notice 655 — 網路衛生控制可以與多項 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 4.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| 4.1 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 4.1 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 4.1 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 4.1 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 4.1 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| 4.1 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 4.1 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 4.1 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 4.1 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 4.1 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| 4.1 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.2 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 4.2 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 4.2 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.2 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 4.2 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項以限制執行個體中繼資料的變更。 |
| 4.2 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.2 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 4.2 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |
| 4.3 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.3 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 4.3 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 4.3 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 4.4 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 4.4 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 4.4 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 4.4 | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 4.4 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 4.4 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 4.4 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 4.4 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 4.4 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 4.4 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 4.4 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 4.4 | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |
| 4.4 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| 4.4 | netfw-policy-default-action-fragment-packets | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包和流量。預設為「傳遞」動作可能會允許非預期的流量。 |
| 4.4 | netfw-policy-default-action-full-packets | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包和流量。預設為「傳遞」動作可能會允許非預期的流量。 |
| 4.4 | netfw-policy-rule-group-associated | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包與流量流程，並定義預設流量處理。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |
| 4.4 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 4.4 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 4.4 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 4.4 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 4.4 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 4.4 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 4.4 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 4.4 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 4.4 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 4.4 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.4 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 4.4 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 4.4 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.5 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 4.5 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 4.5 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.5 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 4.6 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.6 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 4.6 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 4.6 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.6 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 4.6 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

### 範本

該模板可用於 GitHub：MAS 通知 655 的操作最佳實踐。

## MAS TRMG 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了 2021 年 1 月新加坡金融管理局（MAS）技術風險管理指南（TRMG）和託 AWS 管 Config 規則之間的示例映射。每個 AWS Config 規則都適用於特定的 AWS 資源，並與一個或多個 MAS TRMG 控制項相關。MAS 2021 年 1 月的 TRMG 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3.3.1 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 5.4.3 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 5.4.3 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 6.1.1 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 6.1.2 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secre |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | t_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 6.1.4 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 6.1.4 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.1.4 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 6.2.1 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| 6.3.1 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| 6.4.5 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.5 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 6.4.5 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| 6.4.5 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 6.4.5 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 6.4.5 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.5 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 6.4.5 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 6.4.5 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 6.4.5 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 6.4.5 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.5 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 6.4.6 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 6.4.6 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 6.4.6 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.6 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 6.4.6 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.6 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 6.4.6 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.6 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 6.4.6 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.6 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 6.4.7 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 6.4.7 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 6.4.7 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.7 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 6.4.7 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 6.4.7 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 6.4.7 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.7 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 6.4.7 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 6.4.7 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.7 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 6.4.7 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 6.4.7 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.7 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 6.4.7 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 6.4.8 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.8 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 6.4.8 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| 6.4.8 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| 6.4.8 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.8 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| 6.4.8 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4.8 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 7.2.1 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 7.2.1 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.4.1 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 7.4.1 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 7.4.1 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.4.1 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| 7.4.1 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 7.4.1 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.5.5 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |
| 7.5.5 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.5.5 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 7.5.5 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.5.5 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 7.5.5 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 7.5.5 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.5.5 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 7.5.5 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 7.5.5 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 7.5.7 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.5.7 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 7.5.7 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 7.5.7 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 7.5.7 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.5.7 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 7.5.7 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 7.5.7 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.5.7 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 7.5.7 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 7.5.7 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7.5.7 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 8.1.1 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 8.1.1 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.1.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 8.1.1 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| 8.1.1 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| 8.1.1 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.1.1 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 8.1.1 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.1.2 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 8.1.2 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 8.1.2 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.1.2 | opensearch-data-node-fault-tolerance | Amazon OpenSearch 服務 (服 OpenSearch 務) 至少需要三個資料節點才能達到高可用性和容錯能力。部署具有至少三個資料節點的 OpenSearch Service 網域可確保節點失敗時的叢集作業。 |
| 8.1.2 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| 8.1.3 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.1.3 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |
| 8.1.3 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 8.1.3 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 8.4.1 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.4.1 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.4.1 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 8.4.1 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.4.1 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的競爭，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.4.1 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.4.1 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.4.1 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.4.1 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 8.4.1 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 8.4.1 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.4.2 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |
| 8.4.2 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.4.2 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 8.4.2 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.4.2 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的競爭，為 Amazon EBS 磁碟區提供最有效率的效能。 |
| 8.4.2 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.4.2 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.4.2 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.4.2 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 8.4.2 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.4.2 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 8.4.4 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 8.5.4 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 8.5.4 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 9.1.1 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| 9.1.1 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 9.1.1 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 9.1.1 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| 9.1.1 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 9.1.1 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 9.1.1 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 9.1.1 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 9.1.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 9.1.1 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 9.1.1 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 9.1.1 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 9.1.1 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.1 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 9.1.1 | secretsmanager-secret-periodic-rotation | 此規則可確保「 AWS Secrets Manager」密碼已啟用定期輪換。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。預設值為 90 天。 |
| 9.1.1 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.2 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 9.1.2 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.2 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 9.1.2 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.2 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 9.1.2 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 9.1.3 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 9.1.3 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 9.1.3 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.3 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 9.1.3 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 9.1.3 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 9.1.3 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.3 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 9.1.3 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 9.1.3 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 9.1.3 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.3 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 9.1.3 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.3 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 9.1.3 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.3 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 9.1.3 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 9.1.3 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.4 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| 9.1.5 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.5 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 9.1.5 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 9.1.5 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.6 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 9.1.7 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.7 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 9.1.7 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.7 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 9.1.7 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.1.7 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 9.2.1 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 9.2.1 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 9.2.1 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 9.2.1 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.2.1 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 9.2.1 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 9.2.1 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 9.2.1 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.2.1 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 9.2.1 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.2.1 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 9.2.2 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 9.2.2 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 9.2.2 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.2.2 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 9.2.2 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 9.2.2 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.2.2 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 9.2.2 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 9.2.2 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.2.2 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 9.2.2 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.3.1 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 9.3.1 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| 9.3.1 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 9.3.1 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.3.1 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 9.3.1 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 9.3.1 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.3.1 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 9.3.1 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 9.3.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.3.1 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 9.3.1 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 9.3.1 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 9.3.1 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 9.3.1 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.1.1 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 10.1.1 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.1.1 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.1.1 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| 10.1.1 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 10.1.1 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 10.1.1 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 10.1.1 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.1.1 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.1.1 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 10.1.1 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 10.1.1 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.1.1 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.1.1 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 10.1.1 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.1.1 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 10.1.1 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.1.1 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.1.1 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.1.1 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.1.1 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.1.1 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 10.1.1 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 10.1.1 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.1.1 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於敏感資料可靜態存在於 Amazon S3 儲存貯體中，因此請啟用靜態加密以協助保護該資料。 |
| 10.1.1 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 10.1.1 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 10.1.1 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.1.1 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.2.1 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 10.2.1 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 10.2.1 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 10.2.2 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 10.2.3 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 10.2.3 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 10.2.3 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (a) | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 11.1.1 (a) | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.1.1 (a) | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (a) | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (a) | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.1.1 (a) | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.1.1 (a) | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 11.1.1 (a) | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (a) | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.1.1 (a) | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 11.1.1 (b) | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 11.1.1 (b) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 11.1.1 (b) | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.1.1 (b) | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 11.1.1 (b) | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.1.1 (b) | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 11.1.1 (b) | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 11.1.1 (b) | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 11.1.1 (b) | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 11.1.1 (b) | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.1.1 (b) | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 11.1.1 (b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 11.1.1 (b) | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 11.1.1 (b) | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 11.1.1 (b) | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 11.1.1 (b) | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 11.1.1 (b) | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 11.1.1 (b) | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 11.1.1 (b) | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 11.1.1 (b) | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 11.1.1 (b) | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於敏感資料可靜態存在於 Amazon S3 儲存貯體中，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 11.1.1 (b) | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.1 (b) | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.1 (b) | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 11.1.3 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.3 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 11.1.3 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 11.1.3 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.1.3 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.3 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制項會檢查是否有非預期的權限提升。 |
| 11.1.3 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 11.1.3 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 11.1.3 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 11.1.3 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 11.1.3 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 11.1.3 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| 11.1.3 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 11.1.3 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 11.1.3 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 11.1.3 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 11.1.3 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 11.1.3 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.3 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 11.1.3 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 11.1.3 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 11.1.3 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 11.1.3 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於敏感資料可靜態存在於 Amazon S3 儲存貯體中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.1.3 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.3 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 11.1.3 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 11.1.3 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.1 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 11.2.2 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 11.2.2 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.2.2 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.2.2 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.2 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 11.2.2 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 11.2.2 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.2 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 11.2.2 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 11.2.2 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.2 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 11.2.2 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 11.2.2 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 11.2.2 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.2 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 11.2.2 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.2 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 11.2.2 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 11.2.2 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.2 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 11.2.2 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 11.2.2 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 11.2.2 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.2 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 11.2.4 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 11.2.4 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.2.4 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.4 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.2.4 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11.2.4 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.4 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 11.2.4 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 11.2.4 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.4 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 11.2.4 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 11.2.4 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 11.2.4 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.4 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 11.2.4 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.4 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 11.2.4 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 11.2.4 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.4 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 11.2.4 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 11.2.4 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.2.4 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 11.3.1 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| 11.3.5 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.3.5 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 11.3.5 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.3.5 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 11.4.2 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.4.2 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 11.4.2 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 11.4.2 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 11.5.2 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 12.1.1 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 12.1.1 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.1.1 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 12.1.1 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 12.2.2 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.2 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 12.2.2 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 12.2.2 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 12.2.2 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 12.2.2 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.2 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 12.2.2 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 12.2.2 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.2 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 12.2.2 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.2 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 12.2.2 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.2 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 12.2.2 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 12.2.2 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.4 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 12.2.4 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 12.2.5 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.5 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 12.2.5 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.2.5 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 12.3.2 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 12.3.2 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 12.3.2 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.1.2 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 14.1.2 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| 14.1.2 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 14.1.2 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.1.2 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 14.1.2 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 14.1.2 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 14.1.2 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.1.2 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 14.1.3 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 14.1.3 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 14.1.3 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.1.3 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 14.2.2 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 14.2.2 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.2.2 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 14.2.2 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| 14.2.2 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 14.2.2 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 14.2.2 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.2.2 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 14.2.2 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 14.2.2 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 14.2.2 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.2.2 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 14.2.6 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 14.2.6 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 14.2.6 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.2.6 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 14.2.6 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 14.2.6 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 14.2.6 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 14.2.6 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

### 範本

該模板可用於 GitHub：MAS TRMG 的操作最佳實踐。

## 監控的操作最佳實務

此一致性套件包含以內部監視為基礎的 AWS Config 規則。 AWS如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

此範本可在以下網站取得 GitHub：監視的最佳作業作法。

## NBC TRMG 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了柬埔寨國家銀行（NBC）技術風險管理（TRM）指南框架和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 NBC TRM 準則相關。一個 NBC TRM 指導方針可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含柬埔寨國家銀行 (NBC) 技術風險管理 (TRM) 指導方針架構內控制的映射，可在 National Bank of Cambodia: Technology Risk Mangement Guidelines 存取。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(d) | d) 需要考慮的重要控制包括：- 套用和授權建立使用者 ID 和存取控制矩陣的系統化程序 - 進行風險評估並根據結果授予存取權限。- 實作角色型存取控制，旨在確保有效的職責分離 - 變更系統的預設使用者名稱和/或密碼，禁止共用一般帳戶的使用者 ID 和密碼 - 角色或職責一有變更時即修改存取權限，並在僱傭/合約終止時移除存取權限 - 及時通知有關使用者新增、刪除和角色變更之資訊安全功能的程序 - 定期調解系統中的使用者 ID 和必須具有存取權限的實際使用者，並刪除任何不必要的 ID (如果有的話) - 稽核、記錄和監控所有使用者對 IT 資產的存取，以及- 對於長期休假的關鍵應用程式使用者，考慮停用其使用者 ID | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(f) | f) 基於責任目的，請確保可唯一識別使用者和 IT 資產，且其動作是可稽核的。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.1.1(f) | f) 基於責任目的，請確保可唯一識別使用者和 IT 資產，且其動作是可稽核的。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(f) | f) 基於責任目的，請確保可唯一識別使用者和 IT 資產，且其動作是可稽核的。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 3.1.1(f) | f) 基於責任目的，請確保可唯一識別使用者和 IT 資產，且其動作是可稽核的。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 3.1.1(f) | f) 基於責任目的，請確保可唯一識別使用者和 IT 資產，且其動作是可稽核的。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(f) | f) 基於責任目的，請確保可唯一識別使用者和 IT 資產，且其動作是可稽核的。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 3.1.1(f) | f) 基於責任目的，請確保可唯一識別使用者和 IT 資產，且其動作是可稽核的。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | [api-gw-execution-logging-enabled](#) | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1(h) | h) 系統管理員、資安管理人員、程式設計人員以及執行關鍵操作的人員由於其工作職能和特殊權限存取，無可避免地可能會對其所維護或操作的金融系統造成嚴重損害。請務必密切監督具有較高系統存取權限的人員，並記錄其所有系統活動，因為這些人員擁有內部知識和資源，可規避系統控制和安全程序。需要考慮以下列舉的一些控制和安全實務：- 為特殊權限使用者實作雙重要素身分驗證 - 對特殊權限使用者的遠端存取實作強大的控管 - 限制特殊權限使用者的人數 - 基於「必須擁有」或「必須執行」來授予特殊權限存取 - 維護特殊權限使用者所執行系統活動的稽核日誌記錄 - 確保特殊權限使用者無法存取擷取其活動的系統日誌 - 對日誌進行定期稽核或管理檢閱 - 禁止共用特殊權限 ID 及其存取代碼 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | - 禁止供應商和承包商在沒有密切監督和監控的情況下獲得系統的特殊權限存取，以及 - 保護備份資料免於未經授權的存取 | | |
| 3.1.2(a) | a) BFI 應在其 IT 基礎設施的關鍵接合點安裝網路安全裝置 (例如防火牆、防毒/反惡意軟體以及入侵偵測和防護系統)，以保護網路周邊。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 3.1.2(a) | a) BFI 應在其 IT 基礎設施的關鍵接合點安裝網路安全裝置 (例如防火牆、防毒/反惡意軟體以及入侵偵測和防護系統)，以保護網路周邊。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(a) | a) BFI 應在其 IT 基礎設施的關鍵接合點安裝網路安全裝置 (例如防火牆、防毒/反惡意軟體以及入侵偵測和防護系統)，以保護網路周邊。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | [api-gw-execution-logging-enabled](#) | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(c) | c) 應實作控制，以確保網路中的資訊安全，並保護連線服務免於未經授權的存取。具體來說，應考慮以下事項：- 應建立網路設備管理的責任和程序 - 在適當情況下，網路的操作責任應與電腦操作分離 - 應建立特殊控制，以保護透過公有網路或無線網路傳遞之資料的機密性和完整性，並保護連線系統和應用程式 (包括連線至不受信任之系統/網路時的網路加密通訊協定)。- 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作 - 管理活動應緊密協調，以優化提供給組織的服務，並確保將控制一致地應用於整個資訊處理基礎設施 - 網路上的系統應經過驗證，以及 - 應限制不受信任的系統連線至網路 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2(e) | e) 網路服務的範圍可以從簡單的未受管頻寬到複雜的服務 (例如 VPN、Voice over IP、VSAT 等)。網路服務的安全功能應包括：- 應用於網路服務安全的技術，例如驗證、加密和網路連線控制 - 與網路服務進行安全連線所需的技術參數，以符合安全和網路連線規則 - 網路服務使用程序，以在必要時限制對網路服務或應用程式的存取 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(e) | e) 使用加密功能保護遠端存取裝置與機構之間的通訊管道，以限制與網路詐騙有關的風險。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(g) | g) 維護遠端存取通訊的日誌。日誌應包含日期、時間、使用者、使用者位置、持續時間，以及所有遠端存取的目的，包括透過遠端存取進行的所有活動 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 3.1.3(i) | i ) 對遠程訪問強制執行雙因素身份驗證過程（例如，帶有一次性隨機密碼生成器的基於 PIN 的令牌卡或基於令牌的 PKI ） | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(i) | i ) 對遠程訪問強制執行雙因素身份驗證過程（例如，帶有一次性隨機密碼生成器的基於 PIN 的令牌卡或基於令牌的 PKI） | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 3.1.3(i) | i ) 對遠程訪問強制執行雙因素身份驗證過程（例如，帶有一次性隨機密碼生成器的基於 PIN 的令牌卡或基於令牌的 PKI） | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3(i) | i ) 對遠程訪問強制執行雙因素身份驗證過程（例如，帶有一次性隨機密碼生成器的基於 PIN 的令牌卡或基於令牌的 PKI） | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) 修補程式管理程序應包括：-判斷取得及驗證修補程式以確保修補程式來自授權來源的方法-識別適用於組織所使用之應用程式和系統的弱點-評估實施修補程式 (或未實作特定修補程式) 的業務影響-確保修補程式已經過測試-說明部署修補程式的方法，例如自動報告組織的狀態-包括部署修補程式的方法-包括整個組織的部署和方法處理修補程式的部署失敗 (例如，重新部署修補程式)。e) BFIS 應該為所有可用且安全的系統部署自動化修補程式管理工具和軟體更新工具 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) 修補程式管理程序應包括：-判斷取得及驗證修補程式以確保修補程式來自授權來源的方法-識別適用於組織所使用之應用程式和系統的弱點-評估實施修補程式 (或未實作特定修補程式) 的業務影響-確保修補程式已經過測試-說明部署修補程式的方法，例如自動報告組織的狀態-包括部署修補程式的方法-包括整個組織的部署和方法處理修補程式的部署失敗 (例如，重新部署修補程式)。e) BFIS 應該為所有可用且安全的系統部署自動化修補程式管理工具和軟體更新工具 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) 修補程式管理程序應包括：-判斷取得及驗證修補程式以確保修補程式來自授權來源的方法-識別適用於組織所使用之應用程式和系統的弱點-評估實施修補程式 (或未實作特定修補程式) 的業務影響-確保修補程式已經過測試-說明部署修補程式的方法，例如自動報告組織的狀態-包括部署修補程式的方法-包括整個組織的部署和方法處理修補程式的部署失敗 (例如，重新部署修補程式)。e) BFIS 應該為所有可用且安全的系統部署自動化修補程式管理工具和軟體更新工具 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) 修補程式管理程序應包括：-判斷取得及驗證修補程式以確保修補程式來自授權來源的方法-識別適用於組織所使用之應用程式和系統的弱點-評估實施修補程式 (或未實作特定修補程式) 的業務影響-確保修補程式已經過測試-說明部署修補程式的方法，例如自動報告組織的狀態-包括部署修補程式的方法-包括整個組織的部署和方法處理修補程式的部署失敗 (例如，重新部署修補程式)。e) BFIS 應該為所有可用且安全的系統部署自動化修補程式管理工具和軟體更新工具 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) 修補程式管理程序應包括：-判斷取得及驗證修補程式以確保修補程式來自授權來源的方法-識別適用於組織所使用之應用程式和系統的弱點-評估實施修補程式 (或未實作特定修補程式) 的業務影響-確保修補程式已經過測試-說明部署修補程式的方法，例如自動報告組織的狀態-包括部署修補程式的方法-包括整個組織的部署和方法處理修補程式的部署失敗 (例如，重新部署修補程式)。e) BFIS 應該為所有可用且安全的系統部署自動化修補程式管理工具和軟體更新工具 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) 修補程式管理程序應包括：-判斷取得及驗證修補程式以確保修補程式來自授權來源的方法-識別適用於組織所使用之應用程式和系統的弱點-評估實施修補程式 (或未實作特定修補程式) 的業務影響-確保修補程式已經過測試-說明部署修補程式的方法，例如自動報告組織的狀態-包括部署修補程式的方法-包括整個組織的部署和方法處理修補程式的部署失敗 (例如，重新部署修補程式)。e) BFIS 應該為所有可用且安全的系統部署自動化修補程式管理工具和軟體更新工具 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(d)(e) | d) 適當的金鑰管理需要產生、儲存、封存、擷取、分發、淘汰和銷毀密碼編譯金鑰的安全程序 e) 所有密碼編譯金鑰都應受到保護，以免遭到修改和遺失。此外，密碼和私有金鑰需要保護，以防止未經授權的使用及洩漏。用於產生、儲存和封存金鑰的設備應受到實體保護 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 3.1.5(d)(e) | d) 適當的金鑰管理需要產生、儲存、封存、擷取、分發、淘汰和銷毀密碼編譯金鑰的安全程序 e) 所有密碼編譯金鑰都應受到保護，以免遭到修改和遺失。此外，密碼和私有金鑰需要保護，以防止未經授權的使用及洩漏。用於產生、儲存和封存金鑰的設備應受到實體保護 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(d)(e) | d) 適當的金鑰管理需要產生、儲存、封存、擷取、分發、淘汰和銷毀密碼編譯金鑰的安全程序 e) 所有密碼編譯金鑰都應受到保護，以免遭到修改和遺失。此外，密碼和私有金鑰需要保護，以防止未經授權的使用及洩漏。用於產生、儲存和封存金鑰的設備應受到實體保護 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(d)(e) | d) 適當的金鑰管理需要產生、儲存、封存、擷取、分發、淘汰和銷毀密碼編譯金鑰的安全程序 e) 所有密碼編譯金鑰都應受到保護，以免遭到修改和遺失。此外，密碼和私有金鑰需要保護，以防止未經授權的使用及洩漏。用於產生、儲存和封存金鑰的設備應受到實體保護 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(f) | f) 金鑰管理系統應以一套商定的標準、程序和安全方法為基礎：-為不同的加密系統和不同應用程式產生密鑰-發出和取得公開密鑰證書-將密鑰分發給預定的實體，包括如何在收到密鑰時激活-存儲密鑰，包括授權用戶如何獲得密鑰訪問權限-更改或更新密鑰，包括何時應撤銷密鑰的規則以及如何處理密鑰-如何處理密鑰-包括如何鍵應撤回或停用，例如當金鑰遭到入侵或使用者離開組織時 (在此情況下，金鑰也應封存)-復原遺失或損毀的金鑰-備份或歸檔金鑰-銷毀金鑰，以及-記錄和稽核金鑰管理相關活動。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(f) | f) 金鑰管理系統應以一套商定的標準、程序和安全方法為基礎：-為不同的加密系統和不同應用程式產生密鑰-發出和取得公開密鑰證書-將密鑰分發給預定的實體，包括如何在收到密鑰時激活-存儲密鑰，包括授權用戶如何獲得密鑰訪問權限-更改或更新密鑰，包括何時應撤銷密鑰的規則以及如何處理密鑰-如何處理密鑰-包括如何鍵應撤回或停用，例如當金鑰遭到入侵或使用者離開組織時 (在此情況下，金鑰也應封存)-復原遺失或損毀的金鑰-備份或歸檔金鑰-銷毀金鑰，以及-記錄和稽核金鑰管理相關活動。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(f) | f) 金鑰管理系統應以一套商定的標準、程序和安全方法為基礎：-為不同的加密系統和不同應用程式產生密鑰-發出和取得公開密鑰證書-將密鑰分發給預定的實體，包括如何在收到密鑰時激活-存儲密鑰，包括授權用戶如何獲得密鑰訪問權限-更改或更新密鑰，包括何時應撤銷密鑰的規則以及如何處理密鑰-如何處理密鑰-包括如何鍵應撤回或停用，例如當金鑰遭到入侵或使用者離開組織時 (在此情況下，金鑰也應封存)-復原遺失或損毀的金鑰-備份或歸檔金鑰-銷毀金鑰，以及-記錄和稽核金鑰管理相關活動。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(f) | f) 金鑰管理系統應以一套商定的標準、程序和安全方法為基礎：-為不同的加密系統和不同應用程式產生密鑰-發出和取得公開密鑰證書-將密鑰分發給預定的實體，包括如何在收到密鑰時激活-存儲密鑰，包括授權用戶如何獲得密鑰訪問權限-更改或更新密鑰，包括何時應撤銷密鑰的規則以及如何處理密鑰-如何處理密鑰-包括如何鍵應撤回或停用，例如當金鑰遭到入侵或使用者離開組織時 (在此情況下，金鑰也應封存)-復原遺失或損毀的金鑰-備份或歸檔金鑰-銷毀金鑰，以及-記錄和稽核金鑰管理相關活動。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(f) | f) 金鑰管理系統應以一套商定的標準、程序和安全方法為基礎：-為不同的加密系統和不同應用程式產生密鑰-發出和取得公開密鑰證書-將密鑰分發給預定的實體，包括如何在收到密鑰時激活-存儲密鑰，包括授權用戶如何獲得密鑰訪問權限-更改或更新密鑰，包括何時應撤銷密鑰的規則以及如何處理密鑰-如何處理密鑰-包括如何鍵應撤回或停用，例如當金鑰遭到入侵或使用者離開組織時 (在此情況下，金鑰也應封存)-復原遺失或損毀的金鑰-備份或歸檔金鑰-銷毀金鑰，以及-記錄和稽核金鑰管理相關活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(f) | f) 金鑰管理系統應以一套商定的標準、程序和安全方法為基礎：-為不同的加密系統和不同應用程式產生密鑰-發出和取得公開密鑰證書-將密鑰分發給預定的實體，包括如何在收到密鑰時激活-存儲密鑰，包括授權用戶如何獲得密鑰訪問權限-更改或更新密鑰，包括何時應撤銷密鑰的規則以及如何處理密鑰-如何處理密鑰-包括如何鍵應撤回或停用，例如當金鑰遭到入侵或使用者離開組織時 (在此情況下，金鑰也應封存)-復原遺失或損毀的金鑰-備份或歸檔金鑰-銷毀金鑰，以及-記錄和稽核金鑰管理相關活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5(f) | f) 金鑰管理系統應以一套商定的標準、程序和安全方法為基礎：-為不同的加密系統和不同應用程式產生密鑰-發出和取得公開密鑰證書-將密鑰分發給預定的實體，包括如何在收到密鑰時激活-存儲密鑰，包括授權用戶如何獲得密鑰訪問權限-更改或更新密鑰，包括何時應撤銷密鑰的規則以及如何處理密鑰-如何處理密鑰-包括如何鍵應撤回或停用，例如當金鑰遭到入侵或使用者離開組織時 (在此情況下，金鑰也應封存)-復原遺失或損毀的金鑰-備份或歸檔金鑰-銷毀金鑰，以及-記錄和稽核金鑰管理相關活動。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.6(a) | a) BFI 應部署自動化工具和手動技術的組合，以定期執行全方位的 VA。針對以網路為基礎的對外系統，VA 的範圍應包括常見的網路漏洞，例如 SQL 隱碼攻擊和跨網站指令碼攻擊。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.1.6(a) | a) BFI 應部署自動化工具和手動技術的組合，以定期執行全方位的 VA。針對以網路為基礎的對外系統，VA 的範圍應包括常見的網路漏洞，例如 SQL 隱碼攻擊和跨網站指令碼攻擊。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 3.1.6(a) | a) BFI 應部署自動化工具和手動技術的組合，以定期執行全方位的 VA。針對以網路為基礎的對外系統，VA 的範圍應包括常見的網路漏洞，例如 SQL 隱碼攻擊和跨網站指令碼攻擊。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.6(c) | c) BFI 應建立一個程序來修復 VA 與 PT 中識別的問題，並對此修復執行後續重新驗證，以驗證是否完全解決這些缺口。 | vuln-mitigated-accepted (程序檢查) | 確保對新識別的漏洞進行修復，或將其記錄為已接受的風險。應根據您的組織合規要求，對漏洞進行修復或接受其為風險。 |
| 3.1.6(f) | f) 安全功能應提供有關每個部門/分部未緩解重大漏洞數量的狀態更新，並規劃定期提交給資深管理階層進行緩解 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 3.1.8 | 使用者培訓與意識 | security-awareness-program-exists (程序檢查) | 為貴組織建立並維護安全意識計劃。安全意識計畫可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.1.10(b) | b) 敏感資訊，例如系統文件、應用程式原始程式碼和生產交易資料，應具備更廣泛的控制措施來防止變更 (例如完整性檢查程式、密碼編譯雜湊)。此外，政策應盡量減少敏感資訊的分發，包括包含該資訊的列印成品。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 3.2.1(h) | h) 若要將與變更相關的風險降到最低，BFI 應在變更前執行受影響系統或應用程式的備份。如果在部署期間或之後發生問題，BFI 應建立復原計畫，以回復至系統或應用程式的先前版本。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.1(k) | k) 稽核與安全日誌是有助於調查和疑難排解的實用資訊。BFI 應確定已啟用日誌記錄功能，以記錄移轉過程中所執行的活動。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 3.2.3(a) | a) 制定及實作預防、偵測、分析和回應資訊安全事件的程序。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.2.3(a) | a) 制定及實作預防、偵測、分析和回應資訊安全事件的程序。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 3.3.1(a) | a) 將維持高系統可用性、充足容量、可靠效能、快速回應時間、可擴展性等相關重要因素作為系統設計的一部分考量。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | [api-gw-execution-logging-enabled](#) | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) 確保可唯一識別使用者存取記錄，並針對稽核與檢閱目的進行日誌記錄。b) 有責任將識別的未經授權存取記錄在案。c) 對特殊權限使用者所執行的系統活動進行稽核日誌記錄。f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。j) 確保事件日誌記錄奠定了自動化監控系統的基礎，能夠產生有關系統安全的合併報告和提醒。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(f) | f) 應採用適當的日誌記錄和監控，以便記錄和偵測可能影響或與資訊安全有關的動作。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4(g) | g）確保事件日誌包括：-用戶 ID-系統活動-關鍵事件的日期，時間和詳細信息，例如登錄和註銷-設備身份或位置（如果可能的話）和系統標識符-成功和拒絕的系統訪問嘗試的記錄-訪問的文件和其他資源訪問嘗試的記錄-更改系統配置-權限的使用-系統實用程序和應用程序的使用-訪問的文件地址和類型由門禁管制系統提出，以及-用戶在應用程序和在線客戶交易中執行的交易記錄 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 3.6.1(a)(h) | a) BFI 需要確保其 Web 應用程式具有適當的安全措施，並針對各種 Web 安全風險採取合理的緩解措施。h) BFI 需要確保其 Web 應用程式具有適當的安全措施，並針對各種 Web 安全風險採取合理的緩解措施 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1(a)(h) | a) BFI 需要確保其 Web 應用程式具有適當的安全措施，並針對各種 Web 安全風險採取合理的緩解措施。h) BFI 需要確保其 Web 應用程式具有適當的安全措施，並針對各種 Web 安全風險採取合理的緩解措施 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 3.6.1(b) | b) BFI 需要評估與其網際網路銀行系統和其他相關系統有關的安全要求，並考慮所需的機密性和完整性程度以採用加密解決方案。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1(d) | d) 提供網際網路銀行服務的 BFI 必須能夠回應異常的網絡流量情況/系統效能以及系統資源使用率的突然激增，這可能是 DDoS 攻擊的跡象。因此，任何先佔式和被動式行動的成功取決於部署適當的工具，以有效地偵測、監控和分析網路和系統中的異常。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 3.6.1(d) | d) 提供網際網路銀行服務的 BFI 必須能夠回應異常的網絡流量情況/系統效能以及系統資源使用率的突然激增，這可能是 DDoS 攻擊的跡象。因此，任何先佔式和被動式行動的成功取決於部署適當的工具，以有效地偵測、監控和分析網路和系統中的異常。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1(d) | d) 提供網際網路銀行服務的 BFI 必須能夠回應異常的網絡流量情況/系統效能以及系統資源使用率的突然激增，這可能是 DDoS 攻擊的跡象。因此，任何先佔式和被動式行動的成功取決於部署適當的工具，以有效地偵測、監控和分析網路和系統中的異常。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器和 AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.6.1(d) | d) 提供網際網路銀行服務的 BFI 必須能夠回應異常的網絡流量情況/系統效能以及系統資源使用率的突然激增，這可能是 DDoS 攻擊的跡象。因此，任何先佔式和被動式行動的成功取決於部署適當的工具，以有效地偵測、監控和分析網路和系統中的異常。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1(d) | d) 提供網際網路銀行服務的 BFI 必須能夠回應異常的網絡流量情況/系統效能以及系統資源使用率的突然激增，這可能是 DDoS 攻擊的跡象。因此，任何先佔式和被動式行動的成功取決於部署適當的工具，以有效地偵測、監控和分析網路和系統中的異常。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| 3.6.1(e) | e) BFI 需要定期評估資訊安全漏洞，並評估現有 IT 安全風險管理架構的有效性，進行任何必要的調整，以確保及時解決新出現的漏洞。此評估亦應作為任何重大變更的一部分進行。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.6.4(a)(b) | a) 限制網際網路存取，並將關鍵系統與一般 IT 環境隔離。b) 減少受攻擊面和漏洞。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

## 範本

該模板可在以下網站上找到 GitHub：NBC TRMG 的操作最佳實踐。

# NERC CIP BCSI 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了北美電力可靠性公司關鍵基礎設施保護標準 (NERC CIP) 之間的範例映射，包括 BES 網路系統資訊 (BCSI)、CIP-004-7 和 AWS Config CIP-011-3，以及託管規則。每個 AWS Config 規則都會套用至特定 AWS 資源，並與適用於 BCSI 的一或多個 NERC CIP 控制項相關。一個 NERC CIP 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon 網域的最低權限存取。 OpenSearch 它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級的安全性、多租用 OpenSearch 儀表板的支援，以及和 Kibana 的 HTTP 基本驗證。 OpenSearch |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | | |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中，是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | 每個負責實體應實作一或多個經記錄的存取管理計劃，以授權、驗證和撤銷與《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中已識別之「適用系統」有關的 BCSI 已佈建存取，該計劃共同包括《CIP-004-7 表 R6 - BES 網路系統資訊的存取管理》中的每個適用要求部分。若要在此要求情況下被視為具有 BCSI 的存取許可，個人需具備獲得和使用 BCSI 的能力。佈建的存取會被視為為提供個人存取 BCSI 的方法所採取的特定動作所產生的結果 (例如，可能包括實體金鑰或存取卡、使用者和相關的權限和權限、加密金鑰)。第 6.1 部分：在佈建之前，請根據負責實體所確定的需求進行授權 (除非已根據第 4.1 部分授權)，CIP 特殊情況：6.1.1 的情況除外。已將電子存取佈建至電子 BCSI | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記型電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在其加密期間結束後輪換。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | ecr-private-tag-immutability-enabled | 啟用 Elastic Container Repository (ECR) 標籤不變性，防止 ECR 映像上的映像標籤遭到覆寫。先前標籤可能會遭到覆蓋，並需要手動方法來唯一識別映像。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon VPC 內的 Amazon OpenSearch 與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。提醒範例包括：新物件為建立、物件移除、物件還原、遺失和複製的物件。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | s3-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於發佈的訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | rds-cluster-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Relational Database Service (Amazon RDS) 資料庫叢集的受攻擊面。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | rds-instance-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體的受攻擊面。 |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | redshift-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Redshift 叢集的受攻擊面。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | 每個負責實體應實作一或多個經記錄的資訊保護計劃，該計劃共同包括《CIP-011-3 表 R1 - 資訊保護》中的每個適用要求部分。第 1.2 部分：保護和安全處理 BCSI 以減輕外洩機密性風險的方法。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於 Amazon S3 儲存貯體的存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳做法是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |

### 範本

該範本可在以下網站取得 GitHub：NERC CIP BCSI 的營運最佳實務。

## NCSC 雲端安全原則的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供英國國家網路安全中心 (NCSC) 雲端安全原則和 AWS 託管 Config 規則之間的範例對映。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 UK NCSC 雲端安全性原則控制項相關。一個英國 NCSC 雲端安全原則控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含英國 NCSC 雲端安全原則 (National Cyber Security Centre | Cloud security guidance) 控制的映射，這類公共部門資訊根據開放政府授權 (Open Government Licence) 第 3.0 版取得授權。開放政府授權可在此處存取：Open Government Licence for public sector information。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1. 傳輸中的資料保護 | 應充分保護使用者資料傳輸網路，防止遭到篡改和竊聽。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料(以及儲存或處理資料的資產)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2. 資產保護與恢復能力 | 應充分保護您的資料 (以及儲存或處理資料的資產)。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | lambda-dlq-check | 啟用此規則可在函數失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 5. 操作安全 | 服務的運作和管理方式必須能夠阻止、偵測或預防攻擊。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 7. 安全開發 | 雲端服務的設計、開發和部署方式必須能夠盡可能減少並減輕其安全威脅。 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7. 安全開發 | 雲端服務的設計、開發和部署方式必須能夠盡可能減少並減輕其安全威脅。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 7. 安全開發 | 雲端服務的設計、開發和部署方式必須能夠盡可能減少並減輕其安全威脅。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 9. 安全使用者管理 | 供應商應提供工具，以安全管理您對其服務的使用。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | rds-instance-iam-authentication-enabled | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體上啟用 AWS 身分和存取管理 (IAM) 身份驗證，以控制對系統和資產的存取。這會強制使用 Secure Sockets Layer (SSL) 來加密往返資料庫的網路流量。您不需要將使用者憑證放在資料庫，因為身分驗證是由外部管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 10. 身分識別與驗證 | 對服務介面的存取應限制為經過驗證和授權的個人。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | ecs-container-insights-enabled | 監控是維持 Amazon 彈性容器服務 (ECS) 和 AWS 解決方案的可靠性、可用性和效能的重要組成部分。Container Insights 還提供診斷資訊，例如容器重新啟動故障，協助您快速隔離和解決這些故障。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 11. 外部介面保護 | 應識別並防禦所有外部或較不受信任的服務介面。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 12. 安全服務管理 | 雲端供應商應認識到管理系統具有高價值。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 13. 使用者的稽核資訊 | 供應商應提供監控服務存取所需的日誌，以及其中保存的資料。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 13. 使用者的稽核資訊 | 供應商應提供監控服務存取所需的日誌，以及其中保存的資料。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 13. 使用者的稽核資訊 | 供應商應提供監控服務存取所需的日誌，以及其中保存的資料。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 13. 使用者的稽核資訊 | 供應商應提供監控服務存取所需的日誌，以及其中保存的資料。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

## 範本

該模板可用於 GitHub：NCSC 雲安全原則的操作最佳實踐。

# NCSC 網路評估架構的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供英國國家網絡安全中心（NCSC）網絡評估框架（CAF）控制和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則都適用於特定 AWS 資源，並與一個或多個英國 NCSC CAF 控制項相關。一個英國 NCSC CAF 控制可以與多項 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含英國 NCSC CAF (National Cyber Security Centre | NCSC CAF guidance) 內控制的映射，這類公共部門資訊根據開放政府授權 (Open Government Licence) 第 3.0 版取得授權。開放政府授權可在此處存取：Open Government Licence for public sector information。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| A3.a#資產管理 | 對於基本功能運作所需的網路和資訊系統，確定並了解提供、維護或支援這些網路和資訊系統所需的一切項目。這包括資料、人員和系統，以及任何支援的基礎架構 (例如電力或冷卻)。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| A3.a#資產管理 | 對於基本功能運作所需的網路和資訊系統，確定並了解提供、維護或支援這些網路和資訊系統所需的一切項目。這包括資料、人員和系統，以及任何支援的基礎架構 (例如電力或冷卻)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| A3.a#資產管理 | 對於基本功能運作所需的網路和資訊系統，確定並了解提供、維護或支援這些網路和資訊系統所需的一切項目。這包括資料、人員和系統，以及任何支援的基礎架構(例如電力或冷卻)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| A3.a#資產管理 | 對於基本功能運作所需的網路和資訊系統，確定並了解提供、維護或支援這些網路和資訊系統所需的一切項目。這包括資料、人員和系統，以及任何支援的基礎架構(例如電力或冷卻)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| A3.a#資產管理 | 對於基本功能運作所需的網路和資訊系統，確定並了解提供、維護或支援這些網路和資訊系統所需的一切項目。這包括資料、人員和系統，以及任何支援的基礎架構 (例如電力或冷卻)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a#身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.a 身分驗證、驗證及授權 | 您可以對支援基本功能的網路和資訊系統強力確認、驗證並授權其存取。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.b 裝置管理 | 您可以完全了解並信任存取支持基本功能的網路、資訊系統及資料時所使用的裝置。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.b 裝置管理 | 您可以完全了解並信任存取支持基本功能的網路、資訊系統及資料時所使用的裝置。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| B2.c 特殊權限使用者管理 | 您可以密切管理特殊權限使用者對支援基本功能之網路和資訊系統的存取。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B2.d 身分與存取管理 (IdAM) | 對於支援基本功能的網路和資訊系統，您可以為其身分與存取控制提供良好的管理和維護。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| B3.a 了解資料 | 您充分了解哪些資料對於基本功能運作至關重要、其儲存位置、其移動位置，以及無法使用或未經授權的存取、修改或刪除對基本功能造成的不利影響。這也適用於儲存或存取基本功能運作所需重要資料的第三方。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記型電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| B3.b 傳輸中的資料 | 您已保護對基本功能運作至關重要的資料傳輸。這包括將資料傳輸給第三方。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密功能。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的爭用，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| B3.c 儲存的資料 | 您已保護對基本功能運作至關重要的儲存資料。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.a 透過設計保護 | 您可以將安全設計納入支援基本功能運作的網路和資訊系統中。您可以最大程度地減少其受攻擊面，並確保基本功能的運作不會受到任何單一漏洞的惡意探索所影響。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| B4.b 安全組態 | 您可以安全地設定支援基本功能運作的網路和資訊系統。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.b 安全組態 | 您可以安全地設定支援基本功能運作的網路和資訊系統。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| B4.b 安全組態 | 您可以安全地設定支援基本功能運作的網路和資訊系統。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.b 安全組態 | 您可以安全地設定支援基本功能運作的網路和資訊系統。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| B4.c# 安全管理 | 您可以管理支援基本功能運作的組織網路和資訊系統，以實現並維護安全。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.c# 安全管理 | 您可以管理支援基本功能運作的組織網路和資訊系統，以實現並維護安全。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| B4.c# 安全管理 | 您可以管理支援基本功能運作的組織網路和資訊系統，以實現並維護安全。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.d. 漏洞管理 | 您可以管理網路和資訊系統中的已知漏洞，以防止對基本功能造成不良影響。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| B4.d. 漏洞管理 | 您可以管理網路和資訊系統中的已知漏洞，以防止對基本功能造成不良影響。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.d. 漏洞管理 | 您可以管理網路和資訊系統中的已知漏洞，以防止對基本功能造成不良影響。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.d. 漏洞管理 | 您可以管理網路和資訊系統中的已知漏洞，以防止對基本功能造成不良影響。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B4.d. 漏洞管理 | 您可以管理網路和資訊系統中的已知漏洞，以防止對基本功能造成不良影響。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| B4.d. 漏洞管理 | 您可以管理網路和資訊系統中的已知漏洞，以防止對基本功能造成不良影響。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B5.b 彈性設計 | 您可以設計支援基本功能的網路和資訊系統，以抵禦網路安全事件。系統經過適當隔離，資源限制則會放寬。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B5.b 彈性設計 | 您可以設計支援基本功能的網路和資訊系統，以抵禦網路安全事件。系統經過適當隔離，資源限制則會放寬。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B5.b 彈性設計 | 您可以設計支援基本功能的網路和資訊系統，以抵禦網路安全事件。系統經過適當隔離，資源限制則會放寬。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的爭用，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| B5.c 備份 | 對於復原基本功能運作所需的資料和資訊，您持有其目前可存取且安全的備份 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並在 1 分鐘內顯示執行個體的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | lambda-dlq-check | 啟用此規則可在函數失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| C1.a 監控涵蓋範圍 | 您在監控中包含的資料來源可以及時識別可能會影響基本功能運作的安全事件。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| C1.b 保護日誌安全 | 您可以安全地保存日誌記錄資料，並僅向有業務需求的帳戶授予讀取權限。任何員工都不應該在約定的保留期內修改或刪除日誌記錄資料，保留期之後則應將其刪除。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。提醒範例包括：建立新物件、物件移除、物件還原、遺失和複製的物件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | cw-loggroup-retent ion-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| C1.c 產生提醒 | 可靠地識別監控資料中包含潛在安全事件的證據並觸發提醒。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.d 識別安全事件 | 您可以根據威脅和系統的知識將提醒情境化，以識別需要某種形式回應的安全事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| C1.d 識別安全事件 | 您可以根據威脅和系統的知識將提醒情境化，以識別需要某種形式回應的安全事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.e 監控工具與技能 | 監控員工的技能、工具和角色 (包括任何委外的技能、工具和角色) 都應反映控管和報告要求、預期威脅，以及其必須使用的網路或系統資料的複雜性。監控人員了解其必須保護的基本功能。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C1.e 監控工具與技能 | 監控員工的技能、工具和角色 (包括任何委外的技能、工具和角色) 都應反映控管和報告要求、預期威脅，以及其必須使用的網路或系統資料的複雜性。監控人員了解其必須保護的基本功能。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| C1.e 監控工具與技能 | 監控員工的技能、工具和角色 (包括任何委外的技能、工具和角色) 都應反映控管和報告要求、預期威脅，以及其必須使用的網路或系統資料的複雜性。監控人員了解其必須保護的基本功能。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| C2.a 用於攻擊偵測的系統異常 | 您可以定義系統行為異常的範例，提供實用方法來偵測難以識別的惡意活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| C2.a 用於攻擊偵測的系統異常 | 您可以定義系統行為異常的範例，提供實用方法來偵測難以識別的惡意活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| D1.c 測試與練習 | 貴組織使用影響組織 (和其他組織) 的過去事件，以及利用威脅情報和風險評定的情境，進行練習來測試回應計畫。 | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |
| D1.c 測試與練習 | 貴組織使用影響組織 (和其他組織) 的過去事件，以及利用威脅情報和風險評定的情境，進行練習來測試回應計畫。 | response-plan-tested (處理程序檢查) | 確保事件回應和復原計畫都經過測試。這有助於了解計畫在事件期間是否有效，以及是否需要因應任何差距或更新。 |

### 範本

該模板可用於 GitHub：NCSC 網絡評估框架的最佳操作實踐。

## 聯網和內容交付服務的操作最佳實務

此符合性套件包含以網路和內容傳遞服務為基礎的 AWS Config 規則。如需詳細資訊，請參閱上的網路和內容傳遞 AWS。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本位於 GitHub：網路和內容傳遞服務的最佳營運實務。

## NIST 800-53 修訂版 4 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 800-53 與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 NIST 800-53 控制項相關。一個 NIST 800-53 控制項可以與多個 Config 規則相關聯。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

本一致性套件由 AWS 安全保證服務 LLC (AWS SAS) 驗證，該公司是由支付卡產業合格安全評估機構 (QSA)、HITRUST 認證共同安全框架從業人員 (CCSFP) 以及經過認證的合規專業人員組成的團隊，可為各種產業框架提供指導和評估。 AWS SAS 專業人員設計了此一符合性套件，使客戶能夠與 NIST 800-53 的子集保持一致。

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | secretsmanager-scheduled-rotation-success-檢查 | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-user-group-membership-檢查 | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和互聯網安全中心（CIS）AWS 基準密碼強度 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| | | | 基準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | iam-user-unused-credentials-檢查 | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2(1) | 該組織運用自動化機制以支援對資訊系統帳戶的管理。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(3) | 資訊系統會自動停用 [指派: 組織定義的時段] 未經使用的帳戶。 | iam-user-unused-credentials-檢查 | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。CloudTrail 如果啟用多重檔案，則會將日誌檔從所有儲存貯體傳遞 AWS 區域 至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 資訊系統會自動稽核帳戶的建立、修改、啟用、停用和移除動作，並通知 [指派: 組織定義的人員或角色]。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(12)(a) | 組織：a. 監控 [指派: 組織定義的非典型用途] 的資訊系統帳戶。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-2(12)(a) | 組織：a. 監控 [指派: 組織定義的非典型用途] 的資訊系統帳戶。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-user-unused-credentials-檢查 | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和互聯網安全中心（CIS）AWS 基準密碼強度基準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(f) | 組織：f. 根據 [指派: 組織定義的程序或條件] 建立、啟用、修改、停用及移除資訊系統帳戶。 | iam-root-access-key-檢查 | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | S3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶 資訊、IP 地址和事件時間。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AC-2(g) | 組織：g. 監控資訊系統帳戶的使用情況。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | secretsmanager-scheduled-rotation-success-檢查 | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-user-group-membership-檢查 | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和互聯網安全中心（CIS）AWS 基準密碼強度基準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-root-access-key-檢查 | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-group-has-users-檢查 | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(j) | 組織：j. 檢閱帳戶是否符合帳戶管理需求 [指派: 組織定義的頻率]。 | iam-user-no-policies-檢查 | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-user-no-policies-檢查 | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-user-unused-credentials-檢查 | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | S3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-user-group-membership-檢查 | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-root-access-key-檢查 | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-group-has-users-檢查 | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3 | 資訊系統會根據適用的存取控制政策，強制執行已核准的授權，以邏輯存取資訊與系統資源。 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | rds-instance-public-access-檢查 | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為使用邏輯隔離而更加安全。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | vpc-default-security-group-關閉 | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 資訊系統會根據 [指派: 組織定義的資訊流程控制政策] 強制執行已核准的授權，以控制系統內部與互連系統之間的資訊流程。 | internet-gateway-authorized-vpc-只 | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-group-has-users-檢查 | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5c | 組織：c. 定義資訊系統存取授權，以支援職責分離。 | iam-user-no-policies-檢查 | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分獲得或保留過多權限的機會。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | rds-instance-public-access-檢查 | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | S3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | codebuild-project-envvar-awscred-檢查 | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-user-unused-credentials-檢查 | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-group-has-users-檢查 | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-root-access-key-檢查 | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-user-group-membership-檢查 | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。授予使用者超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-user-no-policies-檢查 | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分獲得或保留過多權限的機會。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 組織運用最低權限原則，僅允許授權使用者 (或代表使用者行事流程) 使用根據組織任務和業務職能完成指派任務所必需之存取權。 | iam-no-inline-policy-檢查 | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-6(10) | 資訊系統可防止非特殊權限使用者執行特權功能，包括停用、規避或改變已實作的安全保護/對策。 | iam-root-access-key-檢查 | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| AC-17(1) | 資訊系統監控與控制遠端存取方法。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | S3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | alb-http-drop-invalid-頭啟用 | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(2) | 資訊系統實作密碼編譯機制，以保護遠端存取工作階段的機密性和完整性。 | elb-tls-https-listeners-只 | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(3) | 資訊系統透過 [指派: 組織定義的數目] 個受管網路存取控制點來路由所有遠端存取。 | internet-gateway-authorized-vpc-只 | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | rds-instance-public-access-檢查 | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-21(b) | 組織：b. 運用 [指派: 組織定義的自動化機制或手動程序] 協助使用者決定資訊共用/協同作業。 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | api-gw-execution-logging啟用 | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶 資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。CloudTrail 如果啟用多重檔案，則會將日誌檔從所有儲存貯體傳遞 AWS 區域 至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | S3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2(a)(d) | 組織：a. 確定資訊系統能夠稽核下列事件：[指派: 組織定義的可稽核事件]；d. 確定要在資訊系統內稽核下列事件：[指派: 組織定義的稽核事件 (AU-2 a 中定義的可稽核事件子集)，以及每個已識別事件的稽核頻率 (或需要稽核的情況)]。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | api-gw-execution-logging啟用 | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶 資訊、IP 地址和事件時間。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。CloudTrail 如果啟用多重檔案，則會將日誌檔從所有儲存貯體傳遞 AWS 區域 至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | S3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| AU-3 | 資訊系統產生的稽核記錄會包含下列資訊：建立發生的事件類型、事件發生的時間、事件發生的位置、事件的來源、事件的結果，以及與事件相關聯之任何個人或主體的身分。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU-6(1)(3) | (1) 組織運用自動化機制整合稽核檢閱、分析及報告程序，以支援調查及回應可疑活動的組織程序。(3) 組織會分析不同儲存庫中的稽核記錄並建立彼此的關聯，以獲得全組織的情境感知。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-7(1) | 資訊系統會根據 [指派: 稽核記錄中的組織定義稽核欄位]，讓您能夠處理感興趣事件的稽核記錄。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU-7(1) | 資訊系統會根據 [指派: 稽核記錄中的組織定義稽核欄位]，讓您能夠處理感興趣事件的稽核記錄。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-9 | 資訊系統會保護稽核資訊和稽核工具免於未經授權的存取、修改和刪除。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-9 | 資訊系統會保護稽核資訊和稽核工具免於未經授權的存取、修改和刪除。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| AU-9(2) | 資訊系統每 [指派: 組織定義的頻率] 一次將稽核記錄備份到與所稽核系統或元件實體不同的系統或系統元件上。 | S3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| AU-11 | 組織會保留 [Asset: 組織定義的時段與記錄保留原則一致] 的稽核記錄，以提供安全性事件 after-the-fact 調查的支援，以及符合法規和組織資訊保留需求。 | cw-loggroup-retention-period-檢查 | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | api-gw-execution-logging啟用 | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶 資訊、IP 地址和事件時間。 |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。CloudTrail 如果啟用多重檔案，則會將日誌檔從所有儲存貯體傳遞 AWS 區域 至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。因此，您將收到包含新區域 API 活動的日誌檔，而無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | S3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-12(a)(c) | 資訊系統：a. 在 [指派: 組織定義的資訊系統元件]，為 AU-2 a 中定義的可稽核事件提供稽核記錄產生功能；c. 使用 AU-3 中定義的內容為 AU-2 d 中定義的事件產生稽核記錄。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立適用於監控的 [指派: 組織定義的頻率] 以及適合支援此類監控評估的 [指派: 組織定義的頻率] | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立監控的 [指派: 組織定義的頻率]，以及支援此類監控之評估的 [指派: 組織定義的頻率]。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立監控的 [指派: 組織定義的頻率]，以及支援此類監控之評估的 [指派: 組織定義的頻率]。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立監控的 [指派: 組織定義的頻率]，以及支援此類監控之評估的 [指派: 組織定義的頻率]。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立監控的 [指派: 組織定義的頻率]，以及支援此類監控之評估的 [指派: 組織定義的頻率]。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |
| CA-7(a)(b) | 組織制定了持續監控策略，並實作包括以下內容的持續監控計畫：a. 建立要加以監控的 [指派: 組織定義的指標]；b. 建立監控的 [指派: 組織定義的頻率]，以及支援此類監控之評估的 [指派: 組織定義的頻率]。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-檢managedinstance-association-compliance-status查 | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CM-2 | 組織依組態控制所制定、記錄及維護的目前資訊系統基準組態。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-7(a) | 組織：a. 將資訊系統設定為僅提供基本功能。 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-7(a) | 組織：a. 將資訊系統設定為僅提供基本功能。 | ec2-檢managedinstance-association-compliance-status查 | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(1) | 組織會將資訊系統元件的庫存清單更新為元件安裝、移除和資訊系統更新完整作業之一環。 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-8(3)(a) | 組織：a. 運用自動化機制，依 [指派: 組織定義的頻率] 偵測資訊系統中是否存在未經授權的硬體、軟體和韌體元件 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(3)(a) | 組織：a. 運用自動化機制，依 [指派: 組織定義的頻率] 偵測資訊系統中是否存在未經授權的硬體、軟體和韌體元件 | ec2-檢managedinstance-association-compliance-status查 | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| CM-8(3)(a) | 組織：a. 運用自動化機制，依 [指派: 組織定義的頻率] 偵測資訊系統中是否存在未經授權的硬體、軟體和韌體元件 | ec2-檢managedinstance-patch-compliance-status查 | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | elasticache-redis-cluster-automatic-備份檢查 | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | S3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9(b) | 組織：b. 依 [指派: 與復原時間和復原點目標一致的組織定義頻率] 對資訊系統中包含的系統層級資訊進行備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | S3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | elasticache-redis-cluster-automatic-備份檢查 | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | S3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | elb-cross-zone-load-平衡啟用 | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| CP-10 | 組織能夠在資訊系統中斷、危害或故障之後，恢復及重建到已知狀態。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2 | 資訊系統可唯一識別和驗證組織使用者 (或代表組織使用者行事流程)。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和互聯網安全中心（CIS）AWS 基準密碼強度基準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1)(11) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(11) 資訊系統會針對特殊權限帳戶和非特殊權限帳戶的遠端存取實作多重要素驗證，其中一個要素必須由與取得存取權之系統不同的裝置所提供，且該裝置符合[指派: 組織定義的機制要求強度]。 | root-account-hardware-mfa啟用 | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-2(1)(11) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(11) 資訊系統會針對特殊權限帳戶和非特殊權限帳戶的遠端存取實作多重要素驗證，其中一個要素必須由與取得存取權之系統不同的裝置所提供，且該裝置符合[指派: 組織定義的機制要求強度]。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1)(2)(11) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(2) 資訊系統會針對非特殊權限帳戶的網路存取實作多重要素驗證。(11) 資訊系統會針對特殊權限帳戶和非特殊權限帳戶的遠端存取實作多重要素驗證，其中一個要素必須由與取得存取權之系統不同的裝置所提供，且該裝置符合 [指派: 組織定義的機制要求強度]。 | mfa-enabled-for-iam-控制台訪問 | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA-2(1)(2)(11) | (1) 資訊系統會針對特殊權限帳戶的網路存取實作多重要素驗證。(2) 資訊系統會針對非特殊權限帳戶的網路存取實作多重要素驗證。(11) 資訊系統會針對特殊權限帳戶和非特殊權限帳戶的遠端存取實作多重要素驗證，其中一個要素必須由與取得存取權之系統不同的裝置所提供，且該裝置符合 [指派: 組織定義的機制要求強度]。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(1)(a)(d)(e) | 適用於密碼型驗證的資訊系統：a. 強制執行 [指派: 組織定義的區分大小寫、字元數，以及混合大小寫字母、數字和特殊字元 (包括每種類型的最低要求) 要求] 的最低密碼複雜性；d. 強制執行 [指派: 組織定義的存留期上下限數值] 的密碼存留期上下限；e. 在產生 [指派: 組織定義的次數] 次之後，禁止重複使用密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和互聯網安全中心（CIS）AWS 基準密碼強度基準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(4) | 組織運用自動化工具來判斷密碼驗證器的強度是否足以滿足 [指派: 組織定義的需求]。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和互聯網安全中心（CIS）AWS 基準密碼強度基準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(7) | 組織要確保未加密的靜態驗證器不會嵌入應用程式或存取指令碼中，也不會儲存在功能鍵上。 | codebuild-project-envvar-awscred-檢查 | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| IR-4(1) | 組織會運用自動化機制為事件處理流程提供支援。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-4(1) | 組織會運用自動化機制為事件處理流程提供支援。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| IR-6(1) | 組織會運用自動化機制協助報告安全事件。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-7(1) | 組織會運用自動化機制提高事件回應相關資訊和支援的可用性。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| RA-5 | 組織：a. 掃描資訊系統和託管應用程式中的漏洞 [指派: 組織定義的頻率和/或根據組織定義的程序隨機排列]，以及發現並報告可能影響系統/應用程式的新漏洞時；b. 運用可促進工具間互通性的漏洞掃描工具和技術，並使用以下標準將漏洞管理程序各部分自動化：1. 列舉平台、軟體缺陷和不正確的組態；2. 格式化檢查清單和測試程序；以及 3. 衡量漏洞影響；c. 分析漏洞掃描報告和安全控制評估的結果；d. 依組織的風險評估為據，修補合法漏洞 [指派: 組織定義的回應時間]；以及 e. 與 [指派: 組織定義的人員或角色] 共用從漏洞掃描程序和安全控制評估取得的資訊，以協助消除其他資訊系統中的類似漏洞 (即系統弱點或缺陷)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| RA-5 | 組織：a. 掃描資訊系統和託管應用程式中的漏洞 [指派: 組織定義的頻率和/或根據組織定義的程序隨機排列]，以及發現並報告可能影響系統/應用程式的新漏洞時；b. 運用可促進工具間互通性的漏洞掃描工具和技術，並使用以下標準將漏洞管理程序各部分自動化：1. 列舉平台、軟體缺陷和不正確的組態；2. 格式化檢查清單和測試程序；以及 3. 衡量漏洞影響；c. 分析漏洞掃描報告和安全控制評估的結果；d. 依組織的風險評估為據，修補合法漏洞 [指派: 組織定義的回應時間]；以及 e. 與 [指派: 組織定義的人員或角色] 共用從漏洞掃描程序和安全控制評估取得的資訊，以協助消除其他資訊系統中的類似漏洞 (即系統弱點或缺陷)。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-3(a) | 組織：a. 使用包含資訊安全考量的 [指派: 組織定義的系統開發生命週期] 管理資訊系統。 | codebuild-project-envvar-awscred-檢查 | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SA-3(a) | 組織：a. 使用包含資訊安全考量的 [指派: 組織定義的系統開發生命週期] 管理資訊系統。 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-3(a) | 組織：a. 使用包含資訊安全考量的 [指派: 組織定義的系統開發生命週期] 管理資訊系統。 | codebuild-project-source-repo-網址檢查 | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務 [選取項目 (一或多個): 設計; 開發; 實作; 操作] 期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務 [選取項目 (一或多個): 設計; 開發; 實作; 操作] 期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務 [選取項目 (一或多個): 設計; 開發; 實作; 操作] 期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-10 | 組織要求資訊系統、系統元件或資訊系統服務的開發人員：a. 在系統、元件或服務 [選取項目 (一或多個): 設計; 開發; 實作; 操作] 期間執行組態管理；b. 記錄、管理與控制 [指派: 組態管理下的組織定義組態項目] 變更的完整性；c. 對系統、元件或服務僅實作組織核批准的變更；d. 記錄核准的系統、元件或服務變更，以及此類變更可能造成的安全影響；以及 e. 追蹤系統、元件或服務內的安全缺陷和缺陷解決方案，並向 [指派: 組織定義的人員] 報告調查結果。 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-2 | 資訊系統會將使用者功能 (包括使用者介面服務) 與資訊系統管理功能分開。 | iam-group-has-users-檢查 | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| SC-2 | 資訊系統會將使用者功能 (包括使用者介面服務) 與資訊系統管理功能分開。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-4 | 資訊系統會防止未經授權和意外透過共用系統資源傳輸資訊。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | autoscaling-group-elb-healthcheck-必需 | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | S3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | elb-cross-zone-load-平衡啟用 | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| SC-5 | 資訊系統可運用 [指派: 組織定義的安全防護] 針對下列拒絕服務攻擊類型採取保護措施或限制：[指派: 組織定義的拒絕服務攻擊類型或參考此類資訊的來源]。 | rds-instance-deletion-protection啟用 | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | S3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | elb-tls-https-listeners-只 | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為使用邏輯隔離而更加安全。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | internet-gateway-authorized-vpc-只 | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | rds-instance-public-access-檢查 | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | vpc-default-security-group-關閉 | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | S3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | alb-http-drop-invalid-頭啟用 | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 資訊系統：a. 監控與控制在系統邊界外、系統主要內部邊界內的通訊；b. 實作與內部組織網絡 [選取項目: 實體選取; 邏輯選取] 分開之可公開存取的系統元件子網絡；以及 c. 只能透過受管介面連線至外部網路或資訊系統，這些介面包含依照組織安全架構排列的邊界保護裝置。 | elasticsearch-node-to-node-加密檢查 | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為使用邏輯隔離而更加安全。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | internet-gateway-authorized-vpc-只 | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | ebs-snapshot-public-restorable-檢查 | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | lambda-function-public-access-禁止 | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | rds-instance-public-access-檢查 | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | redshift-cluster-public-access-檢查 | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | 三 account-level-public-access-塊 | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | S3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | S3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | S3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | sagemaker-notebook-no-direct-互聯網接入 | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | vpc-default-security-group-關閉 | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 組織會限制資訊系統的外部網路連線數。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-8 | 資訊系統保護所傳輸資訊的 [選取項目 (一或多個): 機密性; 完整性]。 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的 [選取項目 (一或多個): 機密性; 完整性]。 | alb-http-drop-invalid-頭啟用 | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8 | 資訊系統保護所傳輸資訊的 [選取項目 (一或多個): 機密性; 完整性]。 | elasticsearch-node-to-node-加密檢查 | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的 [選取項目 (一或多個): 機密性; 完整性]。 | elb-tls-https-listeners-只 | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的 [選取項目 (一或多個): 機密性; 完整性]。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8 | 資訊系統保護所傳輸資訊的 [選取項目 (一或多個): 機密性; 完整性]。 | S3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 資訊系統保護所傳輸資訊的 [選取項目 (一或多個): 機密性; 完整性]。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | alb-http-drop-invalid-頭啟用 | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | elasticsearch-node-to-node-加密檢查 | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | elb-tls-https-listeners-只 | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | S3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 除非受到 [指派: 組織定義的替代實體防護] 保護，否則資訊系統會在傳輸過程中實作密碼編譯機制以 [選取項目 (一或多個): 防止未經授權洩漏資訊; 偵測資訊變更]。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-12 | 組織根據 [指派: 組織定義的金鑰產成、分配、儲存、存取和銷毀要求] 為資訊系統中使用的必要密碼編譯建立及管理密碼編譯金鑰。 | cmk-backing-key-rotation啟用 | 啟用金鑰輪換功能，以確保金鑰於加密期間結束後即輪換。 |
| SC-12 | 組織根據 [指派: 組織定義的金鑰產成、分配、儲存、存取和銷毀要求] 為資訊系統中使用的必要密碼編譯建立及管理密碼編譯金鑰。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| SC-12 | 組織根據 [指派: 組織定義的金鑰產成、分配、儲存、存取和銷毀要求] 為資訊系統中使用的必要密碼編譯建立及管理密碼編譯金鑰。 | kms-cmk-not-scheduled-換刪除 | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | api-gw-cache-enabled 和加密 | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | bucket-server-side-encryption啟用 S3- | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | S3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | sagemaker-endpoint-configuration-kms-密鑰配置 | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | sagemaker-notebook-instance-kms-密鑰配置 | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作 [指派: 組織定義的密碼編譯用途及每項用途所需的密碼編譯類型]。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 資訊系統根據適用的聯邦法律、行政命令、指令、政策、法規和標準實作經 FIPS 驗證或 NSA 核准的密碼學。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | alb-http-to-https-重定向檢查 | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | alb-http-drop-invalid-頭啟用 | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23 | 資訊系統會保護通訊工作階段的真確性。 | elb-tls-https-listeners-只 | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | api-gw-cache-enabled 和加密 | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | kms-cmk-not-scheduled-換刪除 | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | S3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | bucket-server-side-encryption啟用 S3- | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | sagemaker-endpoint-configuration-kms-密鑰配置 | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | sagemaker-notebook-instance-kms-密鑰配置 | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 資訊系統會保護 [指派: 組織定義的靜態資訊] 的 [選取項目 (一或多個): 機密性; 完整性]。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-36 | 組織會將 [指派: 組織定義的處理和儲存] 分散到多個實體位置。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-36 | 組織會將 [指派: 組織定義的處理和儲存] 分散到多個實體位置。 | S3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| SI-2(2) | 組織運用自動化機制，依 [指派: 組織定義的頻率] 確定與瑕疵修復有關的資訊系統元件狀態。 | ec2-檢managedinstance-patch-compliance-status查 | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(2) | 組織運用自動化機制，依 [指派: 組織定義的頻率] 確定與瑕疵修復有關的資訊系統元件狀態。 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SI-2(2) | 組織運用自動化機制，依 [指派: 組織定義的頻率] 確定與瑕疵修復有關的資訊系統元件狀態。 | ec2-檢managedinstance-association-compliance-status查 | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(1) | 組織會將個別的入侵偵測工具連入全資訊系統的入侵偵測系統，並加以設定。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI-4(2) | 組織會運用自動化工具支援近乎即時的事件分析。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(4) | 資訊系統會依 [指派: 組織定義的頻率] 監控傳入和傳出通訊流量中是否有異常或未經授權的活動或狀況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI-4(4) | 資訊系統會依 [指派: 組織定義的頻率] 監控傳入和傳出通訊流量中是否有異常或未經授權的活動或狀況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(4) | 資訊系統會依 [指派: 組織定義的頻率] 監控傳入和傳出通訊流量中是否有異常或未經授權的活動或狀況。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4(4) | 資訊系統會依 [指派: 組織定義的頻率] 監控傳入和傳出通訊流量中是否有異常或未經授權的活動或狀況。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4(5) | 發生下列入侵或潛在危害的跡象時，資訊系統會發出警示 [指派: 組織定義的人員或角色]：[指派: 組織定義的入侵指標]。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(16) | 組織會將來自全資訊系統所用監控工具的資訊互相關聯。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | cloud-trail-cloud-watch-日誌啟用 | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | 組織：a. 監控資訊系統以偵測：1. 根據 [指派: 組織定義的監控目標] 劃分的攻擊和潛在攻擊指標；以及 2. 未經授權的本機、網路和遠端連線；b. 識別透過 [指派: 組織定義的技術和方法] 未經授權使用資訊系統；c。部署監控裝置：i. 在資訊系統內以策略方式收集組織決定的重要資訊；以及 (ii) 在系統內的特定位置，追蹤組織感興趣的特定交易類型。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7 | 組織會使用完整性驗證工具來偵測 [指派: 組織定義的軟體、韌體和資訊] 的未經授權變更。 | cloud-trail-log-file-驗證啟用 | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| SI-7(1) | 資訊系統會 [選取項目 (一或多個): 在啟動時; 在 [指派: 組織定義的過渡狀態或安全相關事件] 時; 依 [指派: 組織定義的頻率]] 執行 [指派: 組織定義的軟體、韌體和資訊] 的完整性檢查。 | ec2-instance-managed-by-systems 經理 | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(1) | 資訊系統會 [選取項目 (一或多個): 在啟動時; 在 [指派: 組織定義的過渡狀態或安全相關事件] 時; 依 [指派: 組織定義的頻率]] 執行 [指派: 組織定義的軟體、韌體和資訊] 的完整性檢查。 | ec2-檢managedinstance-patch-compliance-status查 | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SI-7(1) | 資訊系統會 [選取項目 (一或多個): 在啟動時; 在 [指派: 組織定義的過渡狀態或安全相關事件] 時; 依 [指派: 組織定義的頻率]] 執行 [指派: 組織定義的軟體、韌體和資訊] 的完整性檢查。 | cloud-trail-log-file-驗證啟用 | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | S3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | elasticache-redis-cluster-automatic-備份檢查 | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 組織會根據適用的聯邦法律、行政命令、指令、政策、法規、標準和營運要求，處理和保留資訊系統內的資訊以及系統輸出的資訊。 | cw-loggroup-retention-period-檢查 | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

### 範本

該模板可用於 GitHub：NIST 800-53 版本 4 的操作最佳實踐。

## NIST 800-53 修訂版 5 的最佳操作實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 800-53 與 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 NIST 800-53 控制項相關。一個 NIST 800-53 控制項可以與多個 Config 規則相關聯。如需與這些映射相關的詳細資訊和指導，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-2(1) | 帳戶管理 \| 自動化系統帳戶管理 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(3) | 帳戶管理 \| 停用帳戶 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(3) | 帳戶管理 \| 停用帳戶 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(3) | 帳戶管理 \| 停用帳戶 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2(4) | 帳戶管理 \| 自動化稽核動作 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC-2(12) | 帳戶管理 \| 帳戶監控非典型用途 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-2 | 帳戶管理 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-2 | 帳戶管理 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-2 | 帳戶管理 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3(7) | 強制存取 \| 角色型存取控制 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(7) | 強制存取 \| 角色型存取控制 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| AC-3(15) | 強制存取 \| 判別式與強制性存取控制 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC-3 | 強制存取 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |
| AC-3 | 強制存取 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| AC-3 | 強制存取 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-3 | 強制存取 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3 | 強制存取 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC-3 | 強制存取 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3 | 強制存取 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-3 | 強制存取 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-3 | 強制存取 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-3 | 強制存取 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-3 | 強制存取 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-3 | 強制存取 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-3 | 強制存取 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-3 | 強制存取 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3 | 強制存取 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-3 | 強制存取 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-3 | 強制存取 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(21) | 強制執行資訊流程 \| 實體/邏輯分離資訊流程 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC-4(26) | 強制執行資訊流程 \| 稽核篩選動作 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| AC-4 | 強制執行資訊流程 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-4 | 強制執行資訊流程 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| AC-4 | 強制執行資訊流程 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| AC-4 | 強制執行資訊流程 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| AC-4 | 強制執行資訊流程 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| AC-4 | 強制執行資訊流程 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| AC-4 | 強制執行資訊流程 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| AC-4 | 強制執行資訊流程 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 強制執行資訊流程 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 強制執行資訊流程 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-4 | 強制執行資訊流程 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC-4 | 強制執行資訊流程 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-4 | 強制執行資訊流程 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-4 | 強制執行資訊流程 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-4 | 強制執行資訊流程 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-4 | 強制執行資訊流程 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-4 | 強制執行資訊流程 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-4 | 強制執行資訊流程 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-4 | 強制執行資訊流程 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| AC-4 | 強制執行資訊流程 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-4 | 強制執行資訊流程 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-4 | 強制執行資訊流程 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| AC-5 | 職責分離 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5 | 職責分離 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-5 | 職責分離 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5 | 職責分離 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5 | 職責分離 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-5 | 職責分離 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6(2) | 最低權限 \| 非安全功能的非特殊權限存取 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(2) | 最低權限 \| 非安全功能的非特殊權限存取 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6(2) | 最低權限 \| 非安全功能的非特殊權限存取 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(3) | 最低權限 \| 特殊權限命令的網路存取 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-6(3) | 最低權限 \| 特殊權限命令的網路存取 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(3) | 最低權限 \| 特殊權限命令的網路存取 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(3) | 最低權限 \| 特殊權限命令的網路存取 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(3) | 最低權限 \| 特殊權限命令的網路存取 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6(3) | 最低權限 \| 特殊權限命令的網路存取 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(9) | 最低權限 \| 記錄權限功能的使用情形 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AC-6(10) | 最低權限 \| 禁止非特殊權限使用者執行權限功能 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6(10) | 最低權限 \| 禁止非特殊權限使用者執行權限功能 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6(10) | 最低權限 \| 禁止非特殊權限使用者執行權限功能 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| AC-6 | 最低權限 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制項，限制執行個體中繼資料的變更。 |
| AC-6 | 最低權限 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| AC-6 | 最低權限 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| AC-6 | 最低權限 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| AC-6 | 最低權限 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| AC-6 | 最低權限 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-6 | 最低權限 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-6 | 最低權限 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-6 | 最低權限 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6 | 最低權限 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。授予使用者超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| AC-6 | 最低權限 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| AC-6 | 最低權限 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-6 | 最低權限 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-6 | 最低權限 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-6 | 最低權限 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-6 | 最低權限 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-6 | 最低權限 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-6 | 最低權限 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AC-17(2) | 遠端存取 \| 使用加密保護機密性和完整性 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC-17(2) | 遠端存取 \| 使用加密保護機密性和完整性 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(2) | 遠端存取 \| 使用加密保護機密性和完整性 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| AC-17(2) | 遠端存取 \| 使用加密保護機密性和完整性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-17(2) | 遠端存取 \| 使用加密保護機密性和完整性 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-17(2) | 遠端存取 \| 使用加密保護機密性和完整性 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| AC-17(2) | 遠端存取 \| 使用加密保護機密性和完整性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| AC-21 | 共用資訊 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| AC-21 | 共用資訊 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21 | 共用資訊 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21 | 共用資訊 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-21 | 共用資訊 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| AC-21 | 共用資訊 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| AC-21 | 共用資訊 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| AC-21 | 共用資訊 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| AC-21 | 共用資訊 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-21 | 共用資訊 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| AC-21 | 共用資訊 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AC-21 | 共用資訊 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| AU-2 | 事件記錄 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2 | 事件記錄 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU-2 | 事件記錄 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2 | 事件記錄 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU-2 | 事件記錄 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-2 | 事件記錄 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2 | 事件記錄 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-2 | 事件記錄 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-2 | 事件記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2 | 事件記錄 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-2 | 事件記錄 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-2 | 事件記錄 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-2 | 事件記錄 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄內容 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AU-3 | 稽核記錄內容 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄內容 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| AU-3 | 稽核記錄內容 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-3 | 稽核記錄內容 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄內容 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-3 | 稽核記錄內容 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-3 | 稽核記錄內容 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄內容 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-3 | 稽核記錄內容 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄內容 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-3 | 稽核記錄內容 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-3 | 稽核記錄內容 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1) | 檢閱、分析和報告稽核記錄 \| 自動化流程之整合 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-6(1) | 檢閱、分析和報告稽核記錄 \| 自動化流程之整合 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AU-6(1) | 檢閱、分析和報告稽核記錄 \| 自動化流程之整合 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(1) | 檢閱、分析和報告稽核記錄 \| 自動化流程之整合 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-6(3) | 檢閱、分析和報告稽核記錄 \| 建立稽核記錄儲存庫的關聯性 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-6(4) | 檢閱、分析和報告稽核記錄 \| 集中檢閱和分析 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(5) | 檢閱、分析和報告稽核記錄 \| 稽核記錄的整合式分析 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-6(5) | 檢閱、分析和報告稽核記錄 \| 稽核記錄的整合式分析 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| AU-6(5) | 檢閱、分析和報告稽核記錄 \| 稽核記錄的整合式分析 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-6(5) | 檢閱、分析和報告稽核記錄 \| 稽核記錄的整合式分析 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| AU-7(1) | 減少稽核記錄和產生報告 \| 自動處理 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| AU-9(2) | 保護稽核資訊 \| 儲存在不同的實體系統或元件中 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-9(2) | 保護稽核資訊 \| 儲存在不同的實體系統或元件中 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| AU-9(2) | 保護稽核資訊 \| 儲存在不同的實體系統或元件中 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| AU-9(7) | 保護稽核資訊 \| 儲存在不同作業系統的元件中 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-9 | 保護稽核資訊 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| AU-9 | 保護稽核資訊 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-9 | 保護稽核資訊 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-9 | 保護稽核資訊 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| AU-9 | 保護稽核資訊 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-10 | 不可否認性 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| AU-10 | 不可否認性 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-10 | 不可否認性 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| AU-10 | 不可否認性 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-10 | 不可否認性 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-10 | 不可否認性 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-10 | 不可否認性 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-10 | 不可否認性 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-10 | 不可否認性 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU-10 | 不可否認性 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-10 | 不可否認性 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-10 | 不可否認性 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-12 | 產生稽核記錄 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核記錄 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| AU-12 | 產生稽核記錄 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核記錄 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| AU-12 | 產生稽核記錄 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| AU-12 | 產生稽核記錄 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核記錄 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| AU-12 | 產生稽核記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| AU-12 | 產生稽核記錄 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核記錄 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| AU-12 | 產生稽核記錄 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-12 | 產生稽核記錄 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| AU-12 | 產生稽核記錄 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| AU-14(1) | 工作階段稽核 \| 啟動系統 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CA-7 | 持續監控 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| CA-7 | 持續監控 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| CA-7 | 持續監控 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| CA-7 | 持續監控 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。警示範例包括：建立新物件、移除物件、還原物件、遺失和複製物件。 |
| CA-7 | 持續監控 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CA-7 | 持續監控 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| CA-7 | 持續監控 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CA-7 | 持續監控 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| CA-7 | 持續監控 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳號 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CA-7 | 持續監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-7 | 持續監控 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| CA-7 | 持續監控 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | rds-instance-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體的受攻擊面。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | redshift-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Redshift 叢集的受攻擊面。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| CA-9(1) | 內部系統連線 \| 合規性檢查 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2(2) | 基準組態 \| 自動支援準確性和貨幣 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-2(2) | 基準組態 \| 自動支援準確性和貨幣 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2(2) | 基準組態 \| 自動支援準確性和貨幣 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| CM-2(2) | 基準組態 \| 自動支援準確性和貨幣 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CM-2(2) | 基準組態 \| 自動支援準確性和貨幣 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2(2) | 基準組態 \| 自動支援準確性和貨幣 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CM-2 | 基準組態 | account-part-of-organizations | 在 Organizations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | rds-instance-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體的受攻擊面。 |
| CM-2 | 基準組態 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM-2 | 基準組態 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| CM-2 | 基準組態 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| CM-2 | 基準組態 | redshift-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Redshift 叢集的受攻擊面。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-2 | 基準組態 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| CM-3(6) | 組態變更控制 \| 密碼編譯管理 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-3 | 組態變更控制 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| CM-3 | 組態變更控制 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| CM-7 | 最少功能 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-7 | 最少功能 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| CM-7 | 最少功能 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(1) | 清查系統元件 \| 於安裝和移除時更新 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-8(1) | 清查系統元件 \| 於安裝和移除時更新 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(2) | 清查系統元件 \| 自動化維護 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-8(3) | 清查系統元件 \| 自動偵測未經授權的元件 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8(3) | 清查系統元件 \| 自動偵測未經授權的元件 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| CM-8(3) | 清查系統元件 \| 自動偵測未經授權的元件 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| CM-8(3) | 清查系統元件 \| 自動偵測未經授權的元件 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CM-8 | 清查系統元件 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| CM-8 | 清查系統元件 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-2(2) | 緊急應變計畫 \| 規劃容量 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| CP-2(2) | 緊急應變計畫 \| 規劃容量 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(1) | 替代儲存站台 \| 與主站台分離 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6(2) | 替代儲存站台 \| 復原時間和復原點目標 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| CP-6 | 替代儲存站台 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6 | 替代儲存站台 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-6 | 替代儲存站台 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6 | 替代儲存站台 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CP-6 | 替代儲存站台 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-6 | 替代儲存站台 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-6 | 替代儲存站台 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| CP-6 | 替代儲存站台 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9 | 系統備份 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9 | 系統備份 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9 | 系統備份 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-9 | 系統備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CP-9 | 系統備份 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9 | 系統備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| CP-9 | 系統備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CP-9 | 系統備份 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9 | 系統備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| CP-9 | 系統備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-9 | 系統備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| CP-9 | 系統備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 系統復原與重建 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| CP-10 | 系統復原與重建 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| CP-10 | 系統復原與重建 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| CP-10 | 系統復原與重建 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| CP-10 | 系統復原與重建 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| CP-10 | 系統復原與重建 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| CP-10 | 系統復原與重建 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| CP-10 | 系統復原與重建 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| IA-2(1) | 識別與驗證 (組織使用者) \| 特殊特權帳戶的多重要素驗證 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1) | 識別與驗證 (組織使用者) \| 特殊特權帳戶的多重要素驗證 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA-2(1) | 識別與驗證 (組織使用者) \| 特殊特權帳戶的多重要素驗證 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(1) | 識別與驗證 (組織使用者) \| 特殊特權帳戶的多重要素驗證 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-2(2) | 識別與驗證 (組織使用者) \| 非特殊特權帳戶的多重要素驗證 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(2) | 識別與驗證 (組織使用者) \| 非特殊特權帳戶的多重要素驗證 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA-2(2) | 識別與驗證 (組織使用者) \| 非特殊特權帳戶的多重要素驗證 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(2) | 識別與驗證 (組織使用者) \| 非特殊特權帳戶的多重要素驗證 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-2(6) | 識別與驗證 (組織使用者) \| 存取帳戶：不同的裝置 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(6) | 識別與驗證 (組織使用者) \| 存取帳戶：不同的裝置 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA-2(6) | 識別與驗證 (組織使用者) \| 存取帳戶：不同的裝置 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(6) | 識別與驗證 (組織使用者) \| 存取帳戶：不同的裝置 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-2(8) | 識別與驗證 (組織使用者) \| 存取帳戶：阻止重播 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(8) | 識別與驗證 (組織使用者) \| 存取帳戶：阻止重播 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| IA-2(8) | 識別與驗證 (組織使用者) \| 存取帳戶：阻止重播 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-2(8) | 識別與驗證 (組織使用者) \| 存取帳戶：阻止重播 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IA-5(1) | 驗證器管理 \| 密碼式驗證 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| IA-5(7) | 驗證器管理 \| 無嵌入式未加密靜態驗證器 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCES_ID 和 AWS_秘密 _ 碼在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-4(1) | 事件處理 \| 自動化事件處理流程 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| IR-4(5) | 事件處理 \| 自動停用系統 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| RA-3(4) | 風險評估 \| 預測性網路分析 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-3 | 系統開發生命週期 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCES_ID 和 AWS_秘密 _ 碼在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| SA-3 | 系統開發生命週期 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-8(19) | 安全性與隱私權工程原則 \| 持續防護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SA-8(21) | 安全性與隱私權工程原則 \| 自我分析 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SA-8(22) | 安全性與隱私權工程原則 \| 責任與可追蹤性 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-8(25) | 安全性與隱私權工程原則 \| 經濟安全 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SA-11(1) | 開發人員測試與評估 \| 靜態程式碼分析 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SA-11(6) | 開發人員測試與評估 \| 受攻擊面檢閱 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-15(2) | 開發流程、標準和工具 \| 安全性和隱私權追蹤工具 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SA-15(2) | 開發流程、標準和工具 \| 安全性和隱私權追蹤工具 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SA-15(8) | 開發流程、標準和工具 \| 重複使用威脅與漏洞資訊 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SA-15(8) | 開發流程、標準和工具 \| 重複使用威脅與漏洞資訊 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(1) | D enial-of-service 保護 \| 限制攻擊其他系統的能力 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| SC-5(2) | D enial-of-service 保護 \| 容量、頻寬和備援 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-5(3) | D enial-of-service 防護 \| 偵測與監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SC-5 | D enial-of-service 保護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SC-7(3) | 邊界保護 \| 存取點 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| SC-7(3) | 邊界保護 \| 存取點 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(3) | 邊界保護 \| 存取點 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(3) | 邊界保護 \| 存取點 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(3) | 邊界保護 \| 存取點 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(3) | 邊界保護 \| 存取點 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(3) | 邊界保護 \| 存取點 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(3) | 邊界保護 \| 存取點 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(3) | 邊界保護 \| 存取點 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界保護 \| 存取點 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(3) | 邊界保護 \| 存取點 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(3) | 邊界保護 \| 存取點 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(3) | 邊界防護 \| 存取點 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7(4) | 邊界防護 \| 外部電信服務 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(4) | 邊界防護 \| 外部電信服務 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7(5) | 邊界防護 \| 預設拒絕：依例外狀況允許 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(5) | 邊界防護 \| 預設拒絕：依例外狀況允許 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| SC-7(5) | 邊界防護 \| 預設拒絕：依例外狀況允許 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(5) | 邊界防護 \| 預設拒絕：依例外狀況允許 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| SC-7(9) | 邊界防護 \| 限制具威脅性的傳出通訊流量 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(10) | 邊界防護 \| 防止外流 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-7(10) | 邊界防護 \| 防止外流 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| SC-7(10) | 邊界防護 \| 防止外流 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-7(10) | 邊界防護 \| 防止外流 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(10) | 邊界防護 \| 防止外流 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| SC-7(10) | 邊界防護 \| 防止外流 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SC-7(10) | 邊界防護 \| 防止外流 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| SC-7(10) | 邊界防護 \| 防止外流 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(10) | 邊界防護 \| 防止外流 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-7(10) | 邊界防護 \| 防止外流 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(10) | 邊界防護 \| 防止外流 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-7(10) | 邊界防護 \| 防止外流 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(10) | 邊界防護 \| 防止外流 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-7(10) | 邊界防護 \| 防止外流 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SC-7(10) | 邊界防護 \| 防止外流 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(10) | 邊界防護 \| 防止外流 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-7(10) | 邊界防護 \| 防止外流 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| SC-7(10) | 邊界防護 \| 防止外流 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(11) | 邊界防護 \| 限制具威脅性的傳入通訊流量 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(16) | 邊界防護 \| 防止發現系統元件 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(20) | 邊界防護 \| 動態隔離與分隔 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7(21) | 邊界防護 \| 隔離系統元件 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-7 | 邊界防護 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| SC-7 | 邊界防護 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| SC-7 | 邊界防護 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| SC-7 | 邊界防護 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | dms-replication-not-public | 透過確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 邊界防護 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 邊界防護 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7 | 邊界防護 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| SC-7 | 邊界防護 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| SC-7 | 邊界防護 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| SC-7 | 邊界防護 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| SC-7 | 邊界防護 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7 | 邊界防護 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| SC-7 | 邊界防護 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| SC-7 | 邊界防護 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-7 | 邊界防護 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(1) | 傳輸機密性與完整性 \| 密碼編譯防護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8(2) | 傳輸機密性與完整性 \| 傳輸前與傳輸後處理 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 傳輸機密性與完整性 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 傳輸機密性與完整性 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8 | 傳輸機密性與完整性 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 傳輸機密性與完整性 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |
| SC-8 | 傳輸機密性與完整性 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8 | 傳輸機密性與完整性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 傳輸機密性與完整性 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-8 | 傳輸機密性與完整性 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-8 | 傳輸機密性與完整性 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-8 | 傳輸機密性與完整性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-12(2) | 密碼編譯金鑰之建立與管理 \| 對稱金鑰 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC-12(2) | 密碼編譯金鑰之建立與管理 \| 對稱金鑰 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-12(3) | 密碼編譯金鑰之建立與管理 \| 非對稱金鑰 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-12(3) | 密碼編譯金鑰之建立與管理 \| 非對稱金鑰 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-12(3) | 密碼編譯金鑰之建立與管理 \| 非對稱金鑰 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-12(3) | 密碼編譯金鑰之建立與管理 \| 非對稱金鑰 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-12(3) | 密碼編譯金鑰之建立與管理 \| 非對稱金鑰 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-12(3) | 密碼編譯金鑰之建立與管理 \| 非對稱金鑰 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-12(3) | 密碼編譯金鑰之建立與管理 \| 非對稱金鑰 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-12 | 密碼編譯金鑰之建立與管理 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC-12 | 密碼編譯金鑰之建立與管理 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| SC-13 | 密碼編譯防護 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| SC-13 | 密碼編譯防護 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| SC-13 | 密碼編譯防護 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |
| SC-13 | 密碼編譯防護 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-13 | 密碼編譯防護 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-13 | 密碼編譯防護 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC-13 | 密碼編譯防護 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-13 | 密碼編譯防護 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-13 | 密碼編譯防護 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| SC-13 | 密碼編譯防護 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-13 | 密碼編譯防護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-13 | 密碼編譯防護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SC-13 | 密碼編譯防護 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23(3) | 工作階段真實性 \| 唯一由系統產生的工作階段識別符 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23(5) | 工作階段真實性 \| 允許的憑證授權機構 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23(5) | 工作階段真實性 \| 允許的憑證授權機構 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-23 | 工作階段真實性 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23 | 工作階段真實性 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23 | 工作階段真實性 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |
| SC-23 | 工作階段真實性 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23 | 工作階段真實性 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23 | 工作階段真實性 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SC-23 | 工作階段真實性 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SC-23 | 工作階段真實性 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-23 | 工作階段真實性 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-23 | 工作階段真實性 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SC-28(1) | 保護靜態資訊 \| 密碼編譯防護 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28(3) | 保護靜態資訊 \| 密碼編譯金鑰 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| SC-28(3) | 保護靜態資訊 \| 密碼編譯金鑰 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| SC-28 | 保護靜態資訊 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| SC-28 | 保護靜態資訊 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 保護靜態資訊 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 保護靜態資訊 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| SC-28 | 保護靜態資訊 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 保護靜態資訊 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 保護靜態資訊 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SC-28 | 保護靜態資訊 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 保護靜態資訊 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 保護靜態資訊 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SC-28 | 保護靜態資訊 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SC-28 | 保護靜態資訊 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 保護靜態資訊 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SC-28 | 保護靜態資訊 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| SC-28 | 保護靜態資訊 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 保護靜態資訊 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| SC-28 | 保護靜態資訊 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-28 | 保護靜態資訊 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SC-28 | 保護靜態資訊 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SC-28 | 保護靜態資訊 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-36(2) | 分散式處理與儲存 \| 同步 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| SC-36 | 分散式處理與儲存 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| SC-36 | 分散式處理與儲存 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-36 | 分散式處理與儲存 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SC-36 | 分散式處理與儲存 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SI-2(2) | 修補瑕疵 \| 自動化瑕疵修補狀態 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(2) | 修補瑕疵 \| 自動化瑕疵修補狀態 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| SI-2(2) | 修補瑕疵 \| 自動化瑕疵修補狀態 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(3) | 修補瑕疵 \| 修補瑕疵的時間和更正動作基準 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| SI-2(3) | 修補瑕疵 \| 修補瑕疵的時間和更正動作基準 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(3) | 修補瑕疵 \| 修補瑕疵的時間和更正動作基準 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SI-2(4) | 修補瑕疵 \| 自動修補程式管理工具 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| SI-2(4) | 修補瑕疵 \| 自動修補程式管理工具 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(4) | 修補瑕疵 \| 自動修補程式管理工具 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| SI-2(5) | 修補瑕疵 \| 自動更新軟體和韌體 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2(5) | 修補瑕疵 \| 自動更新軟體和韌體 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| SI-2(5) | 修補瑕疵 \| 自動更新軟體和韌體 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2 | 修補瑕疵 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| SI-2 | 修補瑕疵 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2 | 修補瑕疵 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| SI-2 | 修補瑕疵 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2 | 修補瑕疵 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2 | 修補瑕疵 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳號 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| SI-2 | 修補瑕疵 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-2 | 修補瑕疵 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| SI-2 | 修補瑕疵 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。警示範例包括：建立新物件、移除物件、還原物件、遺失和複製物件。 |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-3(8) | 惡意程式碼防護 \| 偵測未經授權的命令 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| SI-4(1) | 系統監控 \| 全系統入侵偵測系統 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(2) | 系統監控 \| 供即時分析的自動化工具和機制 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI-4(4) | 系統監控 \| 傳入和傳出通訊流量 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。警示範例包括：建立新物件、移除物件、還原物件、遺失和複製物件。 |
| SI-4(4) | 系統監控 \| 傳入和傳出通訊流量 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(5) | 系統監控 \| 系統產生的警示 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4(5) | 系統監控 \| 系統產生的警示 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI-4(5) | 系統監控 \| 系統產生的警示 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(12) | 系統監控 \| 將組織產生的警示自動化 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| SI-4(13) | 系統監控 \| 分析流量和事件模式 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(20) | 系統監控 \| 特殊權限使用者 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| SI-4(22) | 系統監控 \| 未授權的網路服務 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4(25) | 系統監控 \| 最佳化網絡流量分析 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| SI-4 | 系統監控 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。警示範例包括：建立新物件、移除物件、還原物件、遺失和複製物件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-4 | 系統監控 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| SI-4 | 系統監控 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(1) | 軟體、韌體和資訊完整性 \| 完整性檢查 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(3) | 軟體、韌體和資訊完整性 \| 集中管理的完整性工具 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連接到 Amazon OpenSearch 服務網域。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| SI-7(6) | 軟體、韌體和資訊完整性 \| 密碼編譯防護 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(7) | 軟體、韌體和資訊完整性 \| 整合偵測與回應 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核能力 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| SI-7(8) | 軟體、韌體和資訊完整性 \| 重大事件稽核功能 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 資訊管理與保留 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SI-12 | 資訊管理與保留 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 資訊管理與保留 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 資訊管理與保留 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |
| SI-12 | 資訊管理與保留 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-12 | 資訊管理與保留 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| SI-12 | 資訊管理與保留 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | s3-version-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-13(5) | 預防可預測的故障 \| 容錯移轉功能 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| SI-20 | 污染 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指導 |
| --- | --- | --- | --- |
| SI-20 | 污染 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| SI-20 | 污染 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

### 範本

該模板可用於 GitHub：NIST 800-53 版本 5 的操作最佳實踐。

## NIST 800 171 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 800-171 與 AWS 受管理 Config 規則之間的對應範例。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 NIST 800-171 控制項相關。一個 NIST 800-171 控制項可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 使用者處理的程序，以及裝置 (包括其他系統)。 | | EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 3.1.1 | 將系統存取限制為授權使用者、代表授權使用者處理的程序，以及裝置 (包括其他系統)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 3.1.2 | 將系統存取限制為授權使用者可執行的交易和功能類型。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 3.1.3 | 根據核准的授權控制 CUI 的流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.1.4 | 個人職責分離可避免勾結，從而降低惡意活動的風險。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 替換為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.1.5 | 採用最低權限的原則，包括用於特定的安全功能和特殊權限帳戶。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.6 | 存取非安全功能時，請使用非特殊權限帳戶或角色。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並稽核此類功能的執行情況。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並稽核此類功能的執行情況。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並稽核此類功能的執行情況。 | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並稽核此類功能的執行情況。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並稽核此類功能的執行情況。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並稽核此類功能的執行情況。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1.7 | 防止非特殊權限使用者執行特殊權限功能，並稽核此類功能的執行情況。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.12 | 監控並控制遠端存取工作階段。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.12 | 監控並控制遠端存取工作階段。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.12 | 監控並控制遠端存取工作階段。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.12 | 監控並控制遠端存取工作階段。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.12 | 監控並控制遠端存取工作階段。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.1.12 | 監控並控制遠端存取工作階段。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.13 | 採用密碼編譯機制來保護遠端存取工作階段的機密性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.14 | 透過受管存取控制點路由遠端存取。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.20 | 驗證並控制/限制與外部系統的連線和使用。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.3.1 | 在所需範圍內建立並保留系統稽核記錄，以便監控、分析、調查和報告非法、未經授權或不恰當的系統活動。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.2 | 確保個別系統使用者的動作可以唯一追蹤到這些使用者，以便使用者能夠對其動作負責。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.4 | 稽核程序失敗時發出警示。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.3.4 | 稽核程序失敗時發出警示。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.5 | 建立稽核檢閱、分析和報告程序的關聯，以供調查並回應不恰當、可疑或異常活動的跡象。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.3.5 | 建立稽核檢閱、分析和報告程序的關聯，以供調查並回應不恰當、可疑或異常活動的跡象。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 3.3.8 | 保護稽核資訊和稽核記錄工具，以防止未經授權的存取、修改和刪除。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存清單 (包括硬體、軟體、韌體及文件)。 | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控庫存清單中未使用的安全群組並管理您的環境。 |
| 3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存清單 (包括硬體、軟體、韌體及文件)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存清單 (包括硬體、軟體、韌體及文件)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存清單 (包括硬體、軟體、韌體及文件)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存清單 (包括硬體、軟體、韌體及文件)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| 3.4.1 | 在各自的系統開發生命週期中，建立並維護組織系統的基準組態和庫存清單 (包括硬體、軟體、韌體及文件)。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有非預期的權限提升。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.4.6 | 透過將組織系統設定為僅提供基本功能，以採用最少功能的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.7 | 限制、停用或禁止使用不必要的程式、功能、連接埠、通訊協定或服務。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.4.7 | 限制、停用或禁止使用不必要的程式、功能、連接埠、通訊協定或服務。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.7 | 限制、停用或禁止使用不必要的程式、功能、連接埠、通訊協定或服務。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 3.4.7 | 限制、停用或禁止使用不必要的程式、功能、連接埠、通訊協定或服務。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.9 | 控制並監控使用者安裝的軟體。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 3.4.9 | 控制並監控使用者安裝的軟體。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織系統的先決條件。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 替換為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |
| 3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織系統的先決條件。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.2 | 驗證 (或確認) 這些使用者、程序或裝置的身分，作為允許存取組織系統的先決條件。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.3 | 使用多重要素驗證對特殊權限帳戶進行本機和網路存取，以及對非特殊權限帳戶進行網路存取。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.5 | 定義期間內禁止重複使用識別符。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.6 | 在定義的閒置期過後停用識別符。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.7 | 建立新密碼時，強制執行最低密碼複雜性和字元變更。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.8 | 在指定的產生次數之後，禁止重複使用密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 3.5.10 | 僅儲存和傳輸以密碼編譯方式保護的密碼。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 3.6.1 | 為組織系統建立營運事件處理功能，包括準備、偵測、分析、遏止、復原和使用者回應活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11.2 | 定期掃描組織系統和應用程式中的漏洞，並在發現影響系統的新漏洞時執行掃描。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.11.2 | 定期掃描組織系統和應用程式中的漏洞，並在發現影響系統的新漏洞時執行掃描。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11.3 | 根據風險評估修補漏洞。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊 (即組織系統傳輸或接收的資訊)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 3.13.1 | 在組織系統的外部邊界和關鍵內部邊界監控、控制及保護通訊(即組織系統傳輸或接收的資訊)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和主體，此類帳戶需要存取控制。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和主體，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.2 | 採用有助於組織系統內有效資訊安全的架構設計、軟體開發技術和系統工程原則。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 3.13.6 | 預設拒絕網路通訊流量，但依例外狀況允許網路通訊流量 (即全部拒絕、依例外狀況允許)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.6 | 預設拒絕網路通訊流量，但依例外狀況允許網路通訊流量 (即全部拒絕、依例外狀況允許)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 3.13.6 | 預設拒絕網路通訊流量，但依例外狀況允許網路通訊流量 (即全部拒絕、依例外狀況允許)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.13.8 | 實作密碼編譯機制，以防止在傳輸過程中未經授權洩漏 CUI (除非受替代實體防護措施保護)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.13.10 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 3.13.10 | 為組織系統中採用的密碼編譯技術建立和管理密碼編譯金鑰。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.16 | 保護靜態 CUI 的機密性。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.16 | 保護靜態 CUI 的機密性。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。因為已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以利保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.16 | 保護靜態 CUI 的機密性。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.16 | 保護靜態 CUI 的機密性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.16 | 保護靜態 CUI 的機密性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.16 | 保護靜態 CUI 的機密性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 3.13.16 | 保護靜態 CUI 的機密性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.14.1 | 及時識別、報告及更正資訊與資訊系統瑕疵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.2 | 在組織系統內的適當位置提供防範惡意程式碼的保護。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.14.2 | 在組織系統內的適當位置提供防範惡意程式碼的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.3 | 監控系統安全提醒和建議，並採取回應行動。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 3.14.4 | 有新版本可用時，請更新惡意程式碼防護機制。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.14.6 | 監控組織系統 (包括傳入和傳出通訊流量)，以偵測攻擊和潛在攻擊的指標。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您將收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.14.7 | 識別未經授權使用組織系統的情況。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

## 範本

該模板可用於 GitHub：NIST 800 171 的操作最佳實踐。

# NIST 800 172 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 800-172 與 AWS 受管 Config 規則之間的對應範例。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 NIST 800-172 控制項相關。一個 NIST 800-172 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | Gateway 的請求進行驗證。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | clb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | ec2-token-hop-limit-check | 確保執行個體中繼資料服務 (IMDS) HTTP PUT 回應僅限於 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。使用 IMDSv2 時，因為中繼資料回應躍點限制設定為 1 (Config 預設值)，所以預設會包含密碼字符的 PUT 回應無法傳送到執行個體之外。如果此值大於 1，則字符可以傳送出 EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1.3e | 使用 [指派：組織定義的安全資訊傳輸解決方案] 來控制已連線系統上安全性網域之間的資訊流程。 | nacl-no-unrestricted-ssh-rdp | 網路存取控制清單 (NACL) 中的遠端伺服器管理連接埠 (例如連接埠 22 (SSH) 和連接埠 3389 (RDP)) 不應可公開存取，因為這可能會允許 VPC 內資源的非預期存取。 |
| 3.2.1e | 提供 [指派：組織定義的頻率] 安全意識訓練，著重於識別和回應來自社交工程、進階持續威脅執行者、違規和可疑行為的威脅；或當威脅發生重大變更時更新 [指派：組織定義的頻率] 訓練。 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |
| 3.4.2e | 使用自動化機制來偵測設定錯誤或未經授權的系統元件；偵測後，[選取 (一或多個)：移除元件；將元件放置在隔離或修復網路中]，以便進行修補、重新設定或其他緩解措施。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.2e | 使用自動化機制來偵測設定錯誤或未經授權的系統元件；偵測後，[選取 (一或多個)：移除元件；將元件放置在隔離或修復網路中]，以便進行修補、重新設定或其他緩解措施。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。保持安裝最新的修補程式是保護系統的最佳實務。 |
| 3.4.2e | 使用自動化機制來偵測設定錯誤或未經授權的系統元件；偵測後，[選取 (一或多個)：移除元件；將元件放置在隔離或修復網路中]，以便進行修補、重新設定或其他緩解措施。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.2e | 使用自動化機制來偵測設定錯誤或未經授權的系統元件；偵測後，[選取 (一或多個)：移除元件；將元件放置在隔離或修復網路中]，以便進行修補、重新設定或其他緩解措施。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| 3.4.3e | 使用自動化探索和管理工具來維護系統元件的完整、準確且隨時可用的清查。 up-to-date | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.3e | 使用自動化探索和管理工具來維護系統元件的完整、準確且隨時可用的清查。 up-to-date | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 3.4.3e | 使用自動化探索和管理工具來維護系統元件的完整、準確且隨時可用的清查。 up-to-date | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4.3e | 使用自動化探索和管理工具來維護系統元件的完整、準確且隨時可用的清查。 up-to-date | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| 3.4.3e | 使用自動化探索和管理工具來維護系統元件的完整、準確且隨時可用的清查。 up-to-date | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.2e | 針對不支援多重要素驗證或複雜帳戶管理的系統和系統元件，使用自動化機制來產生、保護、輪換和管理密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.2e | 針對不支援多重要素驗證或複雜帳戶管理的系統和系統元件，使用自動化機制來產生、保護、輪換和管理密碼。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用期間，並可能降低密碼洩露時所造成的業務影響。 |
| 3.5.2e | 針對不支援多重要素驗證或複雜帳戶管理的系統和系統元件，使用自動化機制來產生、保護、輪換和管理密碼。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| 3.5.2e | 針對不支援多重要素驗證或複雜帳戶管理的系統和系統元件，使用自動化機制來產生、保護、輪換和管理密碼。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |
| 3.11.1e | 使用 [指派：組織定義的威脅情報來源] 作為風險評估的一部分，以引導並通知組織系統的開發、安全架構、安全性解決方案的選擇、監控、威脅追捕，以及回應和復原活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.11.2e | 進行網路威脅追捕活動 [選擇 (一或多個)：[指派：組織定義的頻率]；[指派：組織定義的事件]]，以搜尋 [指派：組織定義的系統] 中的入侵指標，並偵測、追蹤和中斷躲避現有控制的威脅。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.11.5e | 評估 [指派：組織定義的頻率] 安全解決方案的有效性，以根據當前和累積的威脅情報，解決組織系統和組織的預期風險。 | annual-risk-assessment-performed（過程檢查） | 對貴組織執行年度風險評估。風險評估可協助判定已識別風險和/或漏洞影響組織的可能性及影響。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | nacl-no-unrestricted-ssh-rdp | 網路存取控制清單 (NACL) 中的遠端伺服器管理連接埠 (例如連接埠 22 (SSH) 和連接埠 3389 (RDP)) 不應可公開存取，因為這可能會允許 VPC 內資源的非預期存取。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.13.4e | 在組織系統與系統元件中使用 [選取項目: (一或多個)：[指派：組織定義的實體隔離技術]；[指派：組織定義的邏輯隔離技術]]。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 3.14.1e | 使用信任根機制或加密簽署，驗證 [指派：組織定義的安全性關鍵或必要軟體] 的完整性。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.2e | 持續監控組織系統和系統元件的異常或可疑行為。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.14.2e | 持續監控組織系統和系統元件的異常或可疑行為。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 3.14.2e | 持續監控組織系統和系統元件的異常或可疑行為。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.2e | 持續監控組織系統和系統元件的異常或可疑行為。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並在 1 分鐘內顯示執行個體的監控圖形。 |
| 3.14.2e | 持續監控組織系統和系統元件的異常或可疑行為。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.2e | 持續監控組織系統和系統元件的異常或可疑行為。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 3.14.2e | 持續監控組織系統和系統元件的異常或可疑行為。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.6e | 使用從 [指派：組織定義的外部組織] 取得的威脅指示器資訊和有效的緩解措施，以引導並通知入侵偵測和威脅追捕。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3.14.7e | 使用 [指派：組織定義的驗證方法或技術] 驗證 [指派：組織定義的安全性關鍵或必要軟體、韌體和硬體元件] 的正確性。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 3.14.7e | 使用 [指派：組織定義的驗證方法或技術] 驗證 [指派：組織定義的安全性關鍵或必要軟體、韌體和硬體元件] 的正確性。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7e | 使用 [指派：組織定義的驗證方法或技術] 驗證 [指派：組織定義的安全性關鍵或必要軟體、韌體和硬體元件] 的正確性。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 3.14.7e | 使用 [指派：組織定義的驗證方法或技術] 驗證 [指派：組織定義的安全性關鍵或必要軟體、韌體和硬體元件] 的正確性。 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補管理，請更新您的服務獨立任務以使用最新的平台版本。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.14.7e | 使用 [指派：組織定義的驗證方法或技術] 驗證 [指派：組織定義的安全性關鍵或必要軟體、韌體和硬體元件] 的正確性。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存映像的完整性和安全性新增一層驗證。 |

### 範本

該模板可用於 GitHub：NIST 800 172 的操作最佳實踐。

## NIST 800 181 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 800 181 和 AWS 受管 Config 規則之間的範例對應。每個 Config 規則都會套用至特定 AWS 資源，並與一或多個 NIST 800 181 控制項相關。一個 NIST 800 181 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 量，不需限流即可處理突然增加的流量。 |
| T0008 | 分析並規劃資料容量要求的預期變更。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0008 | 分析並規劃資料容量要求的預期變更。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| T0008 | 分析並規劃資料容量要求的預期變更。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| T0008 | 分析並規劃資料容量要求的預期變更。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| T0008 | 分析並規劃資料容量要求的預期變更。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue （Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit （Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0008 | 分析並規劃資料容量要求的預期變更。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰於加密期間結束後即輪換。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | opensearch-encrypted-at-rest | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elasticsearch Service (Amazon ES) 網域啟用加密功能。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0017 | 套用服務導向安全架構原則，以滿足組織的機密性、完整性和可用性要求。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| T0024 | 收集並維護符合系統網路安全報告所需的資料。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| T0042 | 與 Cyber Defense 分析師協調，管理專業網路防禦應用程式的規則和簽章 (例如入侵偵測/保護系統、防毒軟體和內容黑名單) 的更新。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0047 | 建立事件資料關聯以識別特定漏洞，並提出有助於快速修復的建議。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0051 | 根據關鍵系統功能，定義適當的系統可用性層級，並確保系統要求識別適當的災難復原和營運持續性要求，以包含任何適當的容錯移轉/替代站台要求、備份要求，以及系統復原/還原的實質支援能力要求。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| T0065 | 制定並實作網路備份和復原程序。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| T0065 | 制定並實作網路備份和復原程序。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| T0065 | 制定並實作網路備份和復原程序。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| T0065 | 制定並實作網路備份和復原程序。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0065 | 制定並實作網路備份和復原程序。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| T0065 | 制定並實作網路備份和復原程序。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| T0065 | 制定並實作網路備份和復原程序。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| T0065 | 制定並實作網路備份和復原程序。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| T0065 | 制定並實作網路備份和復原程序。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| T0065 | 制定並實作網路備份和復原程序。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| T0065 | 制定並實作網路備份和復原程序。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0065 | 制定並實作網路備份和復原程序。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0070 | 為開發中的系統制定災難復原和營運持續性計畫，並確保在系統進入生產環境之前進行測試。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| T0086 | 確保針對整合到系統設計中商業產品套用的安全修補程式，符合管理機構為預定操作環境所指定的時間表。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0086 | 確保針對整合到系統設計中商業產品套用的安全修補程式，符合管理機構為預定操作環境所指定的時間表。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| T0086 | 確保針對整合到系統設計中商業產品套用的安全修補程式，符合管理機構為預定操作環境所指定的時間表。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0086 | 確保針對整合到系統設計中商業產品套用的安全修補程式，符合管理機構為預定操作環境所指定的時間表。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0110 | 識別和/或確定安全事件是否表示違反法律，而需要採取特定法律行動。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0110 | 識別和/或確定安全事件是否表示違反法律，而需要採取特定法律行動。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| T0110 | 識別和/或確定安全事件是否表示違反法律，而需要採取特定法律行動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0128 | 整合自動化功能，以便在可行的情況下更新或修補系統軟體，並根據系統操作環境目前和預計的修補時間表要求，制定手動更新和修補系統軟體的流程和程序。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| T0128 | 整合自動化功能，以便在可行的情況下更新或修補系統軟體，並根據系統操作環境目前和預計的修補時間表要求，制定手動更新和修補系統軟體的流程和程序。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| T0128 | 整合自動化功能，以便在可行的情況下更新或修補系統軟體，並根據系統操作環境目前和預計的修補時間表要求，制定手動更新和修補系統軟體的流程和程序。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0128 | 整合自動化功能，以便在可行的情況下更新或修補系統軟體，並根據系統操作環境目前和預計的修補時間表要求，制定手動更新和修補系統軟體的流程和程序。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | opensearch-in-vpc-only | 通過確保 Amazon Elasticsearch Service (Amazon ES) 域位於 Amazon Virtual Private Cloud（Amazon VPC）中，以管理對雲的訪問。 AWS Amazon VPC 內的 Amazon ES 網域可在 Amazon VPC 內的 Amazon ES 與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| T0144 | 管理帳戶、網路權限以及系統和設備的存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0151 | 監控並評估企業網路安全防護措施的有效性，以確保其提供預期的保護層級。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0151 | 監控並評估企業網路安全防護措施的有效性，以確保其提供預期的保護層級。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| T0151 | 監控並評估企業網路安全防護措施的有效性，以確保其提供預期的保護層級。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0152 | 監控並維護資料庫以確保最佳效能。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0152 | 監控並維護資料庫以確保最佳效能。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0153 | 監控網路容量和效能。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0153 | 監控網路容量和效能。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| T0153 | 監控網路容量和效能。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0153 | 監控網路容量和效能。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| T0154 | 監控並報告知識管理資產和資源的使用情況。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0156 | 監督並提出有關組態管理的建議。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| T0156 | 監督並提出有關組態管理的建議。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0156 | 監督並提出有關組態管理的建議。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| T0156 | 監督並提出有關組態管理的建議。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0156 | 監督並提出有關組態管理的建議。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| T0156 | 監督並提出有關組態管理的建議。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0156 | 監督並提出有關組態管理的建議。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| T0156 | 監督並提出有關組態管理的建議。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0156 | 監督並提出有關組態管理的建議。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| T0160 | 修補網路漏洞，以確保資訊受到保護免於外界威脅。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0160 | 修補網路漏洞，以確保資訊受到保護免於外界威脅。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| T0160 | 修補網路漏洞，以確保資訊受到保護免於外界威脅。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0162 | 執行資料庫的備份和復原，以確保資料完整性。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| T0166 | 使用從企業內各種來源收集的資訊來執行事件關聯，以獲得情境感知並判斷觀察到的攻擊有效性。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0168 | 根據已建立的資料庫執行雜湊比較。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | opensearch-in-vpc-only | 通過確保 Amazon Elasticsearch Service (Amazon ES) 域位於 Amazon Virtual Private Cloud（Amazon VPC）中，以管理對雲的訪問。 AWS Amazon VPC 內的 Amazon ES 網域可在 Amazon VPC 內的 Amazon ES 與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0195 | 根據任務要求提供相關資訊的受管流程 (透過 Web 型入口網站或其他方式)。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| T0215 | 辨識可能的安全違規，並視需要採取適當的動作來報告事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0244 | 驗證應用程式軟體/網路/系統安全狀態是否按照規定實作、記錄偏差，並建議所需的動作以修正這些偏差。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| T0244 | 驗證應用程式軟體/網路/系統安全狀態是否按照規定實作、記錄偏差，並建議所需的動作以修正這些偏差。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0244 | 驗證應用程式軟體/網路/系統安全狀態是否按照規定實作、記錄偏差，並建議所需的動作以修正這些偏差。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| T0258 | 針對可能的攻擊/入侵、異常活動和濫用活動提供及時偵測、識別和警示，並將這些事件與良性活動區分開來。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0259 | 使用網路防禦工具持續監控和分析系統活動，以識別惡意活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | opensearch-in-vpc-only | 通過確保 Amazon Elasticsearch Service (Amazon ES) 域位於 Amazon Virtual Private Cloud（Amazon VPC）中，以管理對雲的訪問。 AWS Amazon VPC 內的 Amazon ES 網域可在 Amazon VPC 內的 Amazon ES 與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0262 | 採用批准的 defense-in-depth 原則和做法 (例如, defense-in-multiple 地方, 分層防禦, 安全性). | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | opensearch-in-vpc-only | 通過確保 Amazon Elasticsearch Service (Amazon ES) 域位於 Amazon Virtual Private Cloud（Amazon VPC）中，以管理對雲的訪問。 AWS Amazon VPC 內的 Amazon ES 網域可在 Amazon VPC 內的 Amazon ES 與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0284 | 設計並開發與網路安全相關的新工具/技術。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| T0306 | 支援資料庫和資料管理系統的事件管理、服務層級管理、變更管理、發行管理、持續性管理和可用性管理。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0306 | 支援資料庫和資料管理系統的事件管理、服務層級管理、變更管理、發行管理、持續性管理和可用性管理。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| T0306 | 支援資料庫和資料管理系統的事件管理、服務層級管理、變更管理、發行管理、持續性管理和可用性管理。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0314 | 制定系統安全情境、初步系統安全營運概念 (CONOPS)，並根據適用的網路安全要求定義基準系統安全要求。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| T0314 | 制定系統安全情境、初步系統安全營運概念 (CONOPS)，並根據適用的網路安全要求定義基準系統安全要求。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0314 | 制定系統安全情境、初步系統安全營運概念 (CONOPS)，並根據適用的網路安全要求定義基準系統安全要求。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| T0314 | 制定系統安全情境、初步系統安全營運概念 (CONOPS)，並根據適用的網路安全要求定義基準系統安全要求。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| T0314 | 制定系統安全情境、初步系統安全營運概念 (CONOPS)，並根據適用的網路安全要求定義基準系統安全要求。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0314 | 制定系統安全情境、初步系統安全營運概念 (CONOPS)，並根據適用的網路安全要求定義基準系統安全要求。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0333 | 執行網路防禦趨勢分析和報告。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| T0333 | 執行網路防禦趨勢分析和報告。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0347 | 評估來源資料和後續調查結果的有效性。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0358 | 為特殊權限存取使用者設計和開發系統管理功能。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0376 | 根據組織要求，建立、籌資、實作和評估網路人力管理計畫。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0416 | 利用現有的公有金鑰基礎設施 (PKI) 程式庫，並在適當時整合憑證管理和加密功能，以透過公有金鑰啟用應用程式。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0421 | 管理明確組織知識（例如，硬拷貝文檔，數字文件）的索引/編目，存儲和訪問。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | opensearch-in-vpc-only | 通過確保 Amazon Elasticsearch Service (Amazon ES) 域位於 Amazon Virtual Private Cloud（Amazon VPC）中，以管理對雲的訪問。 AWS Amazon VPC 內的 Amazon ES 網域可在 Amazon VPC 內的 Amazon ES 與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0475 | 根據最小特權和原則評估適當的訪問控制 need-to-know. | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| T0489 | 根據既定程序實作系統安全措施，以確保機密性、完整性、可用性、驗證和不可否認性。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0491 | 根據組織標準，為系統使用者安裝並設定硬體、軟體和周邊設備。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| T0491 | 根據組織標準，為系統使用者安裝並設定硬體、軟體和周邊設備。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0491 | 根據組織標準，為系統使用者安裝並設定硬體、軟體和周邊設備。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| T0503 | 監控外部資料來源 (例如網路防禦廠商網站、電腦緊急應變小組、安全焦點)，以維持網路防禦威脅狀況的貨幣，並判斷哪些安全問題可能會對企業產生影響。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0509 | 執行資訊安全風險評估。 | annual-risk-assessment-performed（過程檢查） | 對貴組織執行年度風險評估。風險評估可協助確定已識別風險和/或漏洞影響組織的可能性及影響內容。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | elasticsearch-node-to-node-encryption-check | 確保已 node-to-node 啟用 Amazon Elasticsearch Service 的加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | opensearch-encrypted-at-rest | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elasticsearch Service (Amazon ES) 網域啟用加密功能。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | opensearch-node-to-node-encryption-check | 確保已 node-to-node 啟用 Amazon Elasticsearch Service 的加密。N ode-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | elasticsearch-encrypted-at-rest | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elasticsearch Service (Amazon ES) 網域啟用加密功能。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| T0553 | 套用網路安全功能 (例如加密、存取控制和身分識別管理) 以減少利用機會。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| T0557 | 整合與網路空間相關的主要管理功能。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰於加密期間結束後即輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0557 | 整合與網路空間相關的主要管理功能。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| T0576 | 評估所有來源情報，並建議支援網路營運目標的目標對象。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |
| T0609 | 啟用無線電腦和數位網路的存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | ec2-instance-no-public-ip | 透過確保無法公開存取亞馬遜彈性運算雲端 (Amazon EC2) 執行個體來管理對雲端的存取。 AWS Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon Elasticsearch Service (Amazon ES) 域位於 Amazon Virtual Private Cloud（Amazon VPC）中，以管理對雲的訪問。 AWS Amazon VPC 內的 Amazon ES 網域可在 Amazon VPC 內的 Amazon ES 與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | opensearch-in-vpc-only | 通過確保 Amazon Elasticsearch Service (Amazon ES) 域位於 Amazon Virtual Private Cloud（Amazon VPC）中，以管理對雲的訪問。 AWS Amazon VPC 內的 Amazon ES 網域可在 Amazon VPC 內的 Amazon ES 與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0609 | 啟用無線電腦和數位網路的存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| T0609 | 啟用無線電腦和數位網路的存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| T0616 | 對網路內的系統進行網路偵察和漏洞分析。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0686 | 識別威脅漏洞。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| T0686 | 識別威脅漏洞。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon Elasticsearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| T0706 | 通過傳統和替代技術（例如，社交網絡分析，呼叫鏈接，流量分析）收集有關網絡的信息。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0777 | 分析網路或系統管理員及其活動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0805 | 回報情報衍生的重要網路事件和入侵。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0877 | 與適用的組織單位合作監督取用者資訊存取權限 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| T0935 | 執行資訊安全風險評估。 | annual-risk-assessment-performed（過程檢查） | 對貴組織執行年度風險評估。風險評估可協助確定已識別風險和/或漏洞影響組織的可能性及影響內容。 |
| T0960 | 監控系統及其操作環境的變更。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0960 | 監控系統及其操作環境的變更。 | lambda-dlq-check | 啟用此規則可在功能失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| T0960 | 監控系統及其操作環境的變更。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0960 | 監控系統及其操作環境的變更。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| T0960 | 監控系統及其操作環境的變更。 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0960 | 監控系統及其操作環境的變更。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0960 | 監控系統及其操作環境的變更。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| T0960 | 監控系統及其操作環境的變更。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。（AWS 基礎安全性最佳實踐值：KMS：解密，公里：從）。ReEncrypt 實際值應反映貴組織的政策 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0992 | 確定持續監控結果要如何用於持續授權。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| T0992 | 確定持續監控結果要如何用於持續授權。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰，協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| T0993 | 建立持續監控工具和技術存取控制流程和程序。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

### 範本

該模板可用於 GitHub：NIST 800 181 的操作最佳實踐。

## NIST 1800 25 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 1800-25 與 AWS 受管 Config 規則之間的範例對應。每個都 AWS Config 適用於特定 AWS 資源，並與一個或多個 NIST 1800-25 控制項相關。NIST 1800-25 控制項可以與多個規則相關聯。 AWS Config 如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| ID.RA-1 | 識別和記載資產漏洞 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.RA-1 | 識別和記載資產漏洞 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| ID.RA-1 | 識別和記載資產漏洞 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| ID.RA-1 | 識別和記載資產漏洞 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| PR.AC-3 | 管理遠端存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| PR.AC-3 | 管理遠端存取。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| PR.AC-3 | 管理遠端存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.AC-3 | 管理遠端存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-3 | 管理遠端存取。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-3 | 管理遠端存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-3 | 管理遠端存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.AC-3 | 管理遠端存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-3 | 管理遠端存取。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-3 | 管理遠端存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-3 | 管理遠端存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-3 | 管理遠端存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-3 | 管理遠端存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.AC-3 | 管理遠端存取。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-group-has-users-check | AWS 透過確保 IAM 群組至少有一位使用者，身分與存取權限和存取權限管理 (IAM) 可協助您將最低權限和職責分離的原則整合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-2 | D 受ata-in-transit 到保護 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-2 | D 受ata-in-transit 到保護 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-2 | D 受ata-in-transit 到保護 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-6 | 將完整性檢查機制用於驗證軟體、韌體和資訊完整性 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| PR.DS-6 | 將完整性檢查機制用於驗證軟體、韌體和資訊完整性 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則 (例如功能最小的概念) | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則 (例如功能最小的概念) | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則 (例如功能最小的概念) | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則 (例如功能最小的概念) | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則 (例如功能最小的概念) | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則 (例如功能最小的概念) | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-3 | 施行組態變更控制程序 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| PR.IP-3 | 施行組態變更控制程序 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| PR.IP-9 | 施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | response-plan-exists-maintained (處理程序檢查) | 確保已建立、維護事件回應計畫，並將其分發給負責人員。擁有已更新且正式記載的回應計畫可協助確保回應人員了解事件期間應遵循的角色、責任和程序。 |
| PR.IP-10 | 測試回應和復原計畫。 | response-plan-tested (處理程序檢查) | 確保事件回應和復原計畫都經過測試。這有助於了解計畫在事件期間是否有效，以及是否需要因應任何差距或更新。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-12 | 開發並實作漏洞管理計畫。 | vuln-management-plan-exists (處理程序檢查) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。這可能包括漏洞管理工具、環境掃描頻率、角色和責任。 |
| PR.IP-12 | 開發並實作漏洞管理計畫 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-12 | 開發並實作漏洞管理計畫 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| PR.IP-12 | 開發並實作漏洞管理計畫 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.MA-2 | 以防止未經授權存取的方式核准、記錄及執行組織資產的遠端維護 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| PR.MA-2 | 以防止未經授權存取的方式核准、記錄及執行組織資產的遠端維護 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| PR.PT-1 | 保護通訊和控制網路 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.PT-4 | 保護通訊和控制網路 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| PR.PT-4 | 保護通訊和控制網路 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.PT-4 | 保護通訊和控制網路 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| PR.PT-4 | 保護通訊和控制網路 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-4 | 保護通訊和控制網路 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-4 | 保護通訊和控制網路 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-4 | 保護通訊和控制網路 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.PT-4 | 保護通訊和控制網路 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-4 | 保護通訊和控制網路 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。 Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.PT-4 | 保護通訊和控制網路 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.PT-4 | 保護通訊和控制網路 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-4 | 保護通訊和控制網路 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.PT-4 | 保護通訊和控制網路 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| PR.PT-4 | 保護通訊和控制網路 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| DE.CM-8 | 執行漏洞掃描。 | vuln-scans-performed (處理程序檢查) | 確保根據您的合規需求執行漏洞掃描。貴組織應定義掃描的頻率、使用的工具以及結果的使用方式。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.MI-3 | 對新識別的漏洞進行緩解，或將其記載為已接受的風險。 | vuln-mitigated-accepted (處理程序檢查) | 確保對新識別的漏洞進行修復，或將其記載為已接受的風險。 AWS Security Hub、Amazon 警衛義務、Amazon Inspector 員和 AWS Config 等服務可協助識別環境中的漏洞。應根據您的組織合規要求，對漏洞進行修復或接受其為風險。 |
| RS.MI-3 | 對新識別的漏洞進行緩解，或將其記載為已接受的風險 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

## 範本

該模板可用於 GitHub：NIST 1800 25 的操作最佳實踐。

# NIST CSF 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 網路安全架構 (CSF) 和 AWS 託管 Config 規則之間的範例對應。每個 AWS Config 規則都會套用至特定 AWS 資源，並與一或多個 NIST CSF 控制項相關。一個 NIST CSF 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| DE.AE-1 | 為使用者和系統建立及管理網路操作基準和預期的資料流程 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-2 | 分析偵測到的事件以了解攻擊目標和方法 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| DE.AE-2 | 分析偵測到的事件以了解攻擊目標和方法 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| DE.AE-3 | 從多個來源和感應器收集事件資料並相互關聯 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-4 | 確定事件的影響 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| DE.AE-4 | 確定事件的影響 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| DE.AE-4 | 確定事件的影響 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-4 | 確定事件的影響 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| DE.AE-4 | 確定事件的影響 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-4 | 確定事件的影響 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-4 | 確定事件的影響 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.AE-4 | 確定事件的影響 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。警示範例包括：建立新物件、移除物件、還原物件、遺失和複製物件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| DE.CM-1 | 監控網路以偵測潛在的網路安全事件 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-3 | 監控人員活動以偵測潛在的網路安全事件 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| DE.CM-3 | 監控人員活動以偵測潛在的網路安全事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| DE.CM-3 | 監控人員活動以偵測潛在的網路安全事件 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-3 | 監控人員活動以偵測潛在的網路安全事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-3 | 監控人員活動以偵測潛在的網路安全事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-3 | 監控人員活動以偵測潛在的網路安全事件 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-4 | 偵測到惡意程式碼 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| DE.CM-4 | 偵測到惡意程式碼 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-5 | 偵測到未經授權的行動程式碼 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| DE.CM-5 | 偵測到未經授權的行動程式碼 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| DE.CM-5 | 偵測到未經授權的行動程式碼 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-5 | 偵測到未經授權的行動程式碼 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-5 | 偵測到未經授權的行動程式碼 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| DE.CM-5 | 偵測到未經授權的行動程式碼 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-6 | 監控外部服務供應商活動以偵測潛在的網路安全事件 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| DE.CM-6 | 監控外部服務供應商活動以偵測潛在的網路安全事件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| DE.CM-6 | 監控外部服務供應商活動以偵測潛在的網路安全事件 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-6 | 監控外部服務供應商活動以偵測潛在的網路安全事件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-6 | 監控外部服務供應商活動以偵測潛在的網路安全事件 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-6 | 監控外部服務供應商活動以偵測潛在的網路安全事件 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| DE.CM-7 | 執行監控以找出未經授權的人員、連線、裝置和軟體 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.DP-4 | 傳達事件偵測資訊 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| DE.DP-4 | 傳達事件偵測資訊 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| DE.DP-4 | 傳達事件偵測資訊 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.DP-4 | 傳達事件偵測資訊 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| DE.DP-4 | 傳達事件偵測資訊 | s3-event-notifications-enabled | Amazon S3 事件通知可以在儲存貯體物件發生任何意外或故意修改時提醒相關人員。警示範例包括：建立新物件、移除物件、還原物件、遺失和複製物件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.DP-4 | 傳達事件偵測資訊 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| DE.DP-4 | 傳達事件偵測資訊 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| DE.DP-5 | 持續改善偵測程序 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.AM-2 | 清查組織內的軟體平台和應用程式 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |
| ID.AM-3 | 映射組織通訊和資料流程 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| ID.AM-3 | 映射組織通訊和資料流程 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.AM-3 | 映射組織通訊和資料流程 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| ID.AM-3 | 映射組織通訊和資料流程 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.AM-3 | 映射組織通訊和資料流程 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.AM-3 | 映射組織通訊和資料流程 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| ID.AM-3 | 映射組織通訊和資料流程 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.BE-5 | 對於所有操作狀態（例如，在損壞/攻擊下，恢復期間，正常操作）建立支持關鍵服務交付的恢復性要求 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| ID.RA-1 | 識別和記載資產漏洞 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.RA-1 | 識別和記載資產漏洞 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| ID.RA-1 | 識別和記載資產漏洞 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| ID.RA-1 | 識別和記載資產漏洞 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.RA-2 | 從資訊分享論壇和來源獲得網路威脅情報 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| ID.RA-3 | 識別和記載內部和外部威脅 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| ID.RA-3 | 識別和記載內部和外部威脅 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.RA-5 | 使用威脅、漏洞、可能性影響來確定風險 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| ID.RA-5 | 使用威脅、漏洞、可能性影響來確定風險 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.RA-5 | 使用威脅、漏洞、可能性影響來確定風險 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.RA-5 | 使用威脅、漏洞、可能性影響來確定風險 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| ID.SC-4 | 定期使用稽核、測試結果或其他評估形式來評估供應商和第三方合作夥伴，以確認其履行合約義務。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| ID.SC-4 | 定期使用稽核、測試結果或其他評估形式來評估供應商和第三方合作夥伴，以確認其履行合約義務。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.SC-4 | 定期使用稽核、測試結果或其他評估形式來評估供應商和第三方合作夥伴，以確認其履行合約義務。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| ID.SC-4 | 定期使用稽核、測試結果或其他評估形式來評估供應商和第三方合作夥伴，以確認其履行合約義務。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-1 | 針對授權裝置、使用者和程序核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.AC-3 | 管理遠端存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| PR.AC-3 | 管理遠端存取。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| PR.AC-3 | 管理遠端存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-3 | 管理遠端存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-3 | 管理遠端存取。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-3 | 管理遠端存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.AC-3 | 管理遠端存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-3 | 管理遠端存取。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-3 | 管理遠端存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-3 | 管理遠端存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-3 | 管理遠端存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-3 | 管理遠端存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.AC-3 | 管理遠端存取。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-3 | 管理遠端存取。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-4 | 管理存取許可和授權，並整合最低權限和職責分離的原則 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| PR.AC-5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段） | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-6 | 身分經過證明、繫結至憑證並在互動中宣告 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-6 | 身分經過證明、繫結至憑證並在互動中宣告 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-7 | 使用者、裝置和其他資產經過驗證 (例如，單一因素、多因素)，與交易風險相稱 (例如，個人的安全性與隱私權風險以及其他組織風險) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-7 | 使用者、裝置和其他資產經過驗證 (例如，單一因素、多因素)，與交易風險相稱 (例如，個人的安全性與隱私權風險以及其他組織風險) | iam-user-mfa-enabled | 啟用此規則可限制對 AWS Cloud 資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| PR.AC-7 | 使用者、裝置和其他資產經過驗證 (例如，單一因素、多因素)，與交易風險相稱 (例如，個人的安全性與隱私權風險以及其他組織風險) | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-7 | 使用者、裝置和其他資產經過驗證 (例如，單一因素、多因素)，與交易風險相稱 (例如，個人的安全性與隱私權風險以及其他組織風險) | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| PR.AC-7 | 使用者、裝置和其他資產經過驗證 (例如，單一因素、多因素)，與交易風險相稱 (例如，個人的安全性與隱私權風險以及其他組織風險) | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| PR.AT-1 | 通知並訓練所有使用者 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計畫可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail追蹤已啟用加密功能。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-1 | D 受ata-at-rest 到保護 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-1 | D 受ata-at-rest 到保護 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-2 | D 受ata-in-transit 到保護 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。Node-to-node 加密可為亞馬遜虛擬私人雲端 (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-2 | D 受ata-in-transit 到保護 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-2 | D 受ata-in-transit 到保護 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-2 | D 受ata-in-transit 到保護 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-3 | 資產在整個移除、轉移和處置過程中會受到正式管理 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| PR.DS-3 | 資產在整個移除、轉移和處置過程中會受到正式管理 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-3 | 資產在整個移除、轉移和處置過程中會受到正式管理 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-4 | 維持足夠的容量以確保可用性 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| PR.DS-4 | 維持足夠的容量以確保可用性 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-5 | 實作防止資料洩漏的保護 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.DS-5 | 實作防止資料洩漏的保護 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-6 | 將完整性檢查機制用於驗證軟體、韌體和資訊完整性 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| PR.DS-6 | 將完整性檢查機制用於驗證軟體、韌體和資訊完整性 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-7 | 開發和測試環境會與生產環境分開 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| PR.DS-7 | 開發和測試環境會與生產環境分開 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-7 | 開發和測試環境會與生產環境分開 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| PR.DS-7 | 開發和測試環境會與生產環境分開 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| PR.DS-7 | 開發和測試環境會與生產環境分開 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-7 | 開發和測試環境會與生產環境分開 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則（例如功能最小的概念） | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則（例如功能最小的概念） | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則（例如功能最小的概念） | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則（例如功能最小的概念） | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則（例如功能最小的概念） | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-1 | 資訊科技/工業控制系統的基準配置是建立和維護包含保安原則（例如功能最小的概念） | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| PR.IP-2 | 實作系統開發生命週期來管理系統 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-2 | 實作系統開發生命週期來管理系統 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |
| PR.IP-2 | 實作系統開發生命週期來管理系統 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| PR.IP-3 | 施行組態變更控制程序 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-3 | 施行組態變更控制程序 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| PR.IP-4 | 建立、維護及測試資訊的備份 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-4 | 建立、維護及測試資訊的備份 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| PR.IP-7 | 改善保護程序 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-8 | 分享保護技術的成效 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.IP-8 | 分享保護技術的成效 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.IP-8 | 分享保護技術的成效 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.IP-8 | 分享保護技術的成效 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-8 | 分享保護技術的成效 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| PR.IP-8 | 分享保護技術的成效 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| PR.IP-8 | 分享保護技術的成效 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-8 | 分享保護技術的成效 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.IP-8 | 分享保護技術的成效 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| PR.IP-8 | 分享保護技術的成效 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-8 | 分享保護技術的成效 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.IP-8 | 分享保護技術的成效 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.IP-8 | 分享保護技術的成效 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-12 | 開發並實作漏洞管理計畫 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| PR.IP-12 | 開發並實作漏洞管理計畫 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的受管執行個體指派組態狀態，並可讓您設定作業系統修補程式層級、軟體安裝、應用程式組態，以及環境其他詳細資訊的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.IP-12 | 開發並實作漏洞管理計畫 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| PR.MA-2 | 以防止未經授權存取的方式核准、記錄及執行組織資產的遠端維護 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.MA-2 | 以防止未經授權存取的方式核准、記錄及執行組織資產的遠端維護 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| PR.PT-1 | 保護通訊和控制網路 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。 OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資訊包括存取 Amazon S3 儲存貯體的 AWS 帳戶資訊、IP 地址和事件時間。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| PR.PT-1 | 根據政策確定、記載、實作及檢閱稽核/日誌記錄 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-3 | 將系統設定為僅提供必要功能來整合最少功能的原則 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.PT-4 | 保護通訊和控制網路 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| PR.PT-4 | 保護通訊和控制網路 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.PT-4 | 保護通訊和控制網路 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| PR.PT-4 | 保護通訊和控制網路 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-4 | 保護通訊和控制網路 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-4 | 保護通訊和控制網路 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-4 | 保護通訊和控制網路 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.PT-4 | 保護通訊和控制網路 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-4 | 保護通訊和控制網路 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.PT-4 | 保護通訊和控制網路 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.PT-4 | 保護通訊和控制網路 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-4 | 保護通訊和控制網路 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.PT-4 | 保護通訊和控制網路 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-4 | 保護通訊和控制網路 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| PR.PT-4 | 保護通訊和控制網路 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-5 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RC.RP-1 | 在網路安全事件發生期間或之後執行復原計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| RS.AN-2 | 了解事件的影響 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.MI-3 | 對新識別的漏洞進行緩解，或將其記載為已接受的風險 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| RS.RP-1 | 在事件發生期間或之後執行回應計畫 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

## 範本

該模板可用於 GitHub：NIST CSF 的操作最佳實踐。

# NIST 隱私權架構 1.0 版的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供 NIST 隱私權架構與 AWS 受管 Config 規則之間的範例映射。每個 AWS Config 規則都適用於特定 AWS 資源，並與一或多個 NIST 隱私權架構控制項相關。NIST 隱私權架構控制項可以與多個 AWS Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P7 | 建立並施行處理許可與相關資料值以及資料元素的傳輸機制。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | audit-log-policy-exists(Process Check) | 建立並維護稽核日誌管理原則，以定義組織的日誌記錄需求。這包括但不限於檢閱和保留稽核日誌。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並在 1 分鐘內顯示執行個體的監控圖形。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| CT.DM-P8 | 根據政策並整合資料最小化的原則來確定、記載、實作及檢閱稽核/日誌記錄。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| ID.DE-P2 | 資料處理生態系統當事人 (例如，服務供應商、客戶、合作夥伴、產品製造商、應用程式開發人員) 會使用隱私權風險評估程序來識別、排定優先順序和評估。 | annual-risk-assessment-performed (程序檢查) | 對貴組織執行年度風險評定。風險評定可協助判定已識別風險和/或漏洞影響組織的可能性及影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.AC-P1 | 為授權的個人、程序和裝置核發、管理、驗證、撤銷及稽核身分與憑證。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.AC-P3 | 管理遠端存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-P3 | 管理遠端存取。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-P3 | 管理遠端存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-P3 | 管理遠端存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| PR.AC-P3 | 管理遠端存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| PR.AC-P3 | 管理遠端存取。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| PR.AC-P3 | 管理遠端存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-P3 | 管理遠端存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| PR.AC-P3 | 管理遠端存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-P3 | 管理遠端存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-P3 | 管理遠端存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-P3 | 管理遠端存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.AC-P3 | 管理遠端存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.AC-P3 | 管理遠端存取。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| PR.AC-P3 | 管理遠端存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P3 | 管理遠端存取。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P4 | 管理存取許可和授權，並整合最低權限和職責分離的原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P5 | 網絡完整性受到保護（例如，網絡隔離，網絡分段）。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P6 | 個人和裝置會進行校對並繫結至憑證，並進行驗證，與交易風險相符（例如，個人的安全性和隱私權風險以及其他組織風險）。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P6 | 個人和裝置會進行校對並繫結至憑證，並進行驗證，與交易風險相符（例如，個人的安全性和隱私權風險以及其他組織風險）。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| PR.AC-P6 | 個人和裝置會進行校對並繫結至憑證，並進行驗證，與交易風險相符（例如，個人的安全性和隱私權風險以及其他組織風險）。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.AC-P6 | 個人和裝置會進行校對並繫結至憑證，並進行驗證，與交易風險相符（例如，個人的安全性和隱私權風險以及其他組織風險）。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| PR.AC-P6 | 個人和裝置會進行校對並繫結至憑證，並進行驗證，與交易風險相符（例如，個人的安全性和隱私權風險以及其他組織風險）。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | rds-snapshot-encry pted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P1 | D 受ata-at-rest 到保護。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| PR.DS-P2 | D 受ata-in-transit 到保護。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-P2 | D 受ata-in-transit 到保護。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P2 | D 受ata-in-transit 到保護。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| PR.DS-P2 | D 受ata-in-transit 到保護。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| PR.DS-P2 | D 受ata-in-transit 到保護。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的競爭，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.DS-P4 | 維持足夠的容量以確保可用性。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS _KEY_ID 和 AWS_Secret_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.DS-P5 | 實作防止資料洩漏的保護。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| PR.DS-P6 | 將完整性檢查機制用於驗證軟體、韌體和資訊完整性。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.MA-P2 | 以防止未經授權存取的方式核准、記錄及執行組織資產的遠端維護。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| PR.MA-P2 | 以防止未經授權存取的方式核准、記錄及執行組織資產的遠端維護。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以協助設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未加以刪除，則可能會違反最少功能的概念。 |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| PR.PO-P1 | 資訊技術的基準配置會建立並維護結合安全性原則 (例如，最少功能的概念)。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| AT-1: PR.PO-P10 | 開發並實作漏洞管理計畫。 | vuln-management-plan-exists(Process Check) | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P2 | 建立並施行組態變更控制程序。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| PR.PO-P2 | 建立並施行組態變更控制程序。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的競爭，為 Amazon EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P3 | 建立、維護及測試資訊的備份。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P7 | 建立、施行及管理回應計畫 (事件回應與業務持續性) 和復原計畫 (事件復原與災難復原)。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PO-P8 | 測試回應和復原計畫。 | response-plan-tested(Process Check) | 確保事件回應和復原計畫都經過測試。這有助於了解計畫在事件期間是否有效，以及是否需要因應任何差距或更新。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| PR.PT-P2 | 將系統設定為僅提供必要功能來整合最少功能的原則。 | redshift-enhanced-vpc-routing-enabled | 增強型 VPC 路由會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過 Amazon VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。也可以使用 VPC 流程日誌來監控網路流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| PR.PT-P3 | 保護通訊和控制網路。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-P3 | 保護通訊和控制網路。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-P3 | 保護通訊和控制網路。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-P3 | 保護通訊和控制網路。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| PR.PT-P3 | 保護通訊和控制網路。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| PR.PT-P3 | 保護通訊和控制網路。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| PR.PT-P3 | 保護通訊和控制網路。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| PR.PT-P3 | 保護通訊和控制網路。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| PR.PT-P3 | 保護通訊和控制網路。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| PR.PT-P3 | 保護通訊和控制網路。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| PR.PT-P3 | 保護通訊和控制網路。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| PR.PT-P3 | 保護通訊和控制網路。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| PR.PT-P3 | 保護通訊和控制網路。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| PR.PT-P3 | 保護通訊和控制網路。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P3 | 保護通訊和控制網路。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力需求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點已設定最短保留期。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| PR.PT-P4 | 實作機制 (例如，故障安全防護、負載平衡、熱抽換)，以在正常和不利情況下達到彈性需求。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，使您能夠符合業務與法規的備份合規要求。。 |

## 範本

該模板可用於 GitHub：NIST 隱私框架 v1.0 的操作最佳實踐。

# NYDFS 23 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了紐約州金融服務部（NYDFS）針對金融服務公司（23 NYCRR 500）的網絡安全要求和 AWS 託管 Config 規則之間的示例映射。每個 AWS Config 規則都適用於特定 AWS 資源，並與一個或多個美國 NYDFS 控制項相關。美國 NYDFS 23 NYCRR 500 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | 護涵蓋實體資訊系統的機密性、完整性和可用性。 | | 啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，進而導致應用程式喪失可用性。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果發生基礎架構失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能靜態存在敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道來設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式處理一或多個執行個體遺失的能力。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，進而導致應用程式喪失可用性。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未進行回報，流量就會傳送到新的 Amazon EC2 執行個體。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告提供狀態描述項，以評估已識別問題的嚴重性，並找出可能的調查原因。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並在 1 分鐘內顯示執行個體的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.02(a) | (a) 網路安全計畫。每個涵蓋實體應維護網路安全計畫，旨在保護涵蓋實體資訊系統的機密性、完整性和可用性。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 500.02(b)(2) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(2) 使用防禦性基礎架構與政策和程序的實作來保護涵蓋實體的資訊系統，以及儲存在這些資訊系統中的非公開資訊，防範未經授權的存取、使用或其他惡意行為。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並在 1 分鐘內顯示執行個體的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每個裝置的資料，以及次要主機指標。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 500.02(b)(3) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(3) 偵測網路安全事件。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化藉由減少 Amazon EBS I/O 操作與執行個體的其他流量之間的競爭，為 Amazon EBS 磁碟區提供最有效率的效能。 |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆地從意外的使用者動作和應用程式失敗中復原。 |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | backup-plan-min-frequency-and-min-retention-check | 為協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| 500.02(b)(5) | (b) 網路安全計畫應以涵蓋實體的風險評估為基礎，並設計用於執行下列核心網路安全功能：(5) 從網路安全事件復原並還原正常操作和服務。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.05 | 每個涵蓋實體的網路安全計畫應包括根據涵蓋實體的風險評估開發的監控和測試，設計用來評估涵蓋實體的網路安全計畫的有效性。監控和測試應包括持續監控或定期滲透測試和漏洞評估。如果缺乏有效的持續監控或其他系統以持續偵測可能產生或指出漏洞的資訊系統變更，涵蓋實體應：(a) 每年根據風險評估中已識別的相關風險，對涵蓋實體的資訊系統進行年度滲透測試；以及 (b) 每兩年進行一次漏洞評估，包括任何系統掃描或資訊系統檢閱，其目的旨在根據風險評估識別涵蓋實體資訊系統中的網路安全漏洞。 | vuln-management-plan-exists（過程檢查） | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(b) | (b) 每個涵蓋實體應將本部分第 500.06(a)(1) 節所要求的記錄至少保存五年，且應將本部分第 500.06(a)(2) 節所要求的紀錄至少保存三年。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.06(a) | (a) 每個涵蓋實體應在適用範圍內，根據其風險評估安全地維護系統：(1) 設計用來重建足以支援涵蓋實體正常作業和義務的重大財務交易；以及 (2) 包括設計用來偵測和回應網路安全事件的稽核記錄，這些網路安全事件很可能會對涵蓋實體正常作業的任何重要部分造成重大損害。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | ecs-task-definition-user-for-host-mode-check | 如果任務定義具有更高的權限，這是因為客戶已特別選擇使用這些組態。當任務定義已啟用主機網路，但客戶尚未選擇使用更高的權限時，此控制會檢查是否有意外的權限提升。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環功能。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 500.07 | 作為其網路安全計畫的一部分，根據涵蓋實體的風險評估，每個涵蓋實體應限制使用者對可存取非公開資訊之資訊系統的存取權限，並應定期檢閱此類存取權限。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.8(a) | (a) 每個涵蓋實體的網路安全計畫應包括旨在確保為涵蓋實體使用的內部開發應用程式使用安全開發實務的書面程序、指南和標準，以及在涵蓋實體技術環境範圍內針對涵蓋實體所用外部開發應用程式的安全性進行評估、評定或測試的程序。 | codebuild-project-envvar-awscred-check | 請確定驗證認證 AW_ACCESS_KEY_ID 和 AWS_SECRET_KEY 在程式碼建置專案環境中不存在。 AWS 請勿將這些變數儲存為純文字。以純文字格式儲存這些變數會導致非預期的資料暴露和未經授權的存取。 |
| 500.8(a) | (a) 每個涵蓋實體的網路安全計畫應包括旨在確保為涵蓋實體使用的內部開發應用程式使用安全開發實務的書面程序、指南和標準，以及在涵蓋實體技術環境範圍內針對涵蓋實體所用外部開發應用程式的安全性進行評估、評定或測試的程序。 | codebuild-project-source-repo-url-check | 確保 GitHub 或 Bitbucket 源存儲庫 URL 不包含個人訪問令牌， AWS Codebuild 項目環境中的登錄憑據。使用 OAuth 而不是個人訪問令牌或登錄憑據來授予訪問 GitHub 或 Bitbucket 存儲庫的授權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.09 | (a) 每個涵蓋實體均應定期對涵蓋實體的資訊系統進行風險評估，足以根據本部分的要求為網路安全計畫的設計提供資訊。此類風險評估應根據合理需求進行更新，以因應涵蓋實體資訊系統、非公開資訊或業務營運的變更。涵蓋實體的風險評估應允許對控制進行修訂，以因應技術發展和不斷發展的威脅，並應考慮涵蓋實體的業務營運與網路安全、收集或儲存的非公開資訊、使用的資訊系統，以及用來保護非公開資訊和資訊系統之控制其可用性和有效性相關的特定風險。 | annual-risk-assessment-performed (處理程序檢查) > | 對貴組織執行年度風險評估。風險評估可協助判定已識別風險和/或漏洞影響組織的可能性及影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.12 | (a) 多重要素驗證。根據其風險評估，每個涵蓋實體應使用有效的控制，其中可能包括多重要素驗證或以風險為基礎的驗證，以防止未經授權存取非公開資訊或資訊系統。(b) 對於任何從外部網路存取涵蓋實體內部網路的個人均應使用多重要素驗證，除非涵蓋實體的資訊安全長以書面形式核准使用適當等效或更安全的存取控制。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 500.12 | (a) 多重要素驗證。根據其風險評估，每個涵蓋實體應使用有效的控制，其中可能包括多重要素驗證或以風險為基礎的驗證，以防止未經授權存取非公開資訊或資訊系統。(b) 對於任何從外部網路存取涵蓋實體內部網路的個人均應使用多重要素驗證，除非涵蓋實體的資訊安全長以書面形式核准使用適當等效或更安全的存取控制。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.12 | (a) 多重要素驗證。根據其風險評估，每個涵蓋實體應使用有效的控制，其中可能包括多重要素驗證或以風險為基礎的驗證，以防止未經授權存取非公開資訊或資訊系統。(b) 對於任何從外部網路存取涵蓋實體內部網路的個人均應使用多重要素驗證，除非涵蓋實體的資訊安全長以書面形式核准使用適當等效或更安全的存取控制。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 500.12 | (a) 多重要素驗證。根據其風險評估，每個涵蓋實體應使用有效的控制，其中可能包括多重要素驗證或以風險為基礎的驗證，以防止未經授權存取非公開資訊或資訊系統。(b) 對於任何從外部網路存取涵蓋實體內部網路的個人均應使用多重要素驗證，除非涵蓋實體的資訊安全長以書面形式核准使用適當等效或更安全的存取控制。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.12 | (a) 多重要素驗證。根據其風險評估，每個涵蓋實體應使用有效的控制，其中可能包括多重要素驗證或以風險為基礎的驗證，以防止未經授權存取非公開資訊或資訊系統。(b) 對於任何從外部網路存取涵蓋實體內部網路的個人均應使用多重要素驗證，除非涵蓋實體的資訊安全長以書面形式核准使用適當等效或更安全的存取控制。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | cloudwatch-alarm-action-check | 當指標違反指定數量評估期間的閾值時，Amazon 會發出 CloudWatch 警示。警示會根據在數個期間與閾值相關的指標值或表達式值來執行一或多個動作。此規則需要 alarmActionRequired (Config 預設值：True)、insufficientDataAction 必要 (Config 預設值：True)、 okActionRequired (Config 預設值：False) 的值。實際值應反映您環境的警示動作。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。憑藉 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。請建置輸出日誌提供有關組建專案的詳細資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| 500.14(a) | (a) 實作以風險為基礎的政策、程序和控制，旨在監控授權使用者的活動，並偵測這類授權使用者對非公開資訊的未經授權存取、使用或竄改。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.14(b) | 作為其網路安全計畫的一部分，每個涵蓋實體應：(b) 為所有人員提供定期的網路安全意識訓練，該訓練會進行更新以反映涵蓋實體在其風險評估中識別的風險。 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計畫可教育員工如何保護其組織免於遭受各種安全漏洞或事件侵害。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | encrypted-volumes | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統對來自 API Gateway 的請求進行驗證。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能靜態存在敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 500.15(a) | (a) 作為其網路安全計畫的一部分，根據其風險評估，每個涵蓋實體應實作控制 (包括加密)，以保護涵蓋實體在透過外部網路傳輸中和靜態持有的非公開資訊。 | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 500.16 | (a) 作為其網路安全計畫的一部分，每個涵蓋實體應制定書面事件回應計畫，旨在迅速回應嚴重影響涵蓋實體資訊系統的機密性、完整性或可用性，或涵蓋實體業務或作業所有層面之持續功能的網路安全事件，並從這些事件中復原。 | response-plan-exists-maintained （過程檢查） | 確保已建立、維護事件回應計畫，並將其分發給負責人員。 |

### 範本

該模板可用於 GitHub：NYDFS 23 的操作最佳實踐。

## NZISM 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供紐西蘭政府通訊安全局 (GCSB) 資訊安全手冊 (NZISM) 2022-09 版 3.6 與受管 Config 規則之間的對映範例。 AWS 每個 Config 規則都適用於特定 AWS 資源，並與一個或多個 NZISM 控制項相

關。一個 NZISM 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

此一致性套件範本範例包含 NZISM 架構控制的映射，該架構是保護安全要求 (PSR) 架構不可或缺的一部分，其中闡述了紐西蘭政府對人員、資訊和實體安全管理的期望。

NZISM 依據 Creative Commons 姓名標示 4.0 紐西蘭授權條款獲得授權，這些授權條款可從 https://creativecommons.org/licenses/by/4.0/ 取得。如需著作權資訊，請參閱 NZISM New Zealand Information Security Manual | Legal, Privacy, and Copyrigh。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1149 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1149 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 1149 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| 1149 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 1149 | ec2-hardening-and-state-management（過程檢查） | 強化的 EC2 伺服器映像建置程序與狀態管理員關聯已設定為移除不需要的元件和服務，並安裝反惡意軟體和日誌代理程式。 |
| 1661 | cloudfront-default-root-object-configured | 此控制項會檢查 Amazon CloudFront 分發是否設定為傳回預設根物件的特定物件。如果 CloudFront 散佈沒有設定預設根物件，則控制項會失敗。使用者有時可能會請求提供分佈的根 URL，而不是分佈中的物件。發生這種情況時，指定預設根物件可協助避免暴露 Web 分佈的內容。您必須在 us-east-1 區域中套用此規則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1667 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 1667 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1841 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 1841 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1841 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1841 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 1847 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1847 | cloudfront-viewer-policy-https | 此控制項會檢查 Amazon CloudFront 分發是否要求檢視者直接使用 HTTPS，或是否使用重新導向。如果針對快取行為設定 ViewerProtocolPolicy 為允許全部 defaultCacheBehavior 或控制項，則控制項會失敗。HTTPS (TLS) 可用來協助防止潛在攻擊者利用 person-in-the-middle 或類似攻擊來竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。您必須在 us-east-1 區域中套用此規則。 |
| 1847 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1847 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1847 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1858 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1893 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 1893 | federate-with-central-idp (處理程序檢查) | 需要存取 AWS 資源的人力身分識別會使用與 SSO 聯合的中央 IdP 進行驗證。 AWS 中央 IdP 會在 3 次嘗試登入失敗後鎖定系統使用者。 |
| 1946 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1946 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| 1998 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| 1998 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 1998 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 2013 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2013 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 2013 | cloudfront-accesslogs-enabled | 此控制項會檢查是否已在 CloudFront 分發上啟用伺服器存取記錄。如果未針對分佈啟用存取日誌記錄，則此控制會失敗。CloudFront 訪問日誌提供有關 CloudFront 接收的每個用戶請求的詳細信息。每個日誌都包含收到請求的日期和時間、提出請求的檢視者 IP 地址、請求的來源，以及檢視者提出請求的連接埠號碼等資訊。這些日誌適用於安全與存取稽核及鑑識調查等應用程式。您必須在 us-east-1 區域中套用此規則。 |
| 2013 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2013 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 2013 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 2022 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2022 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 2028 | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |
| 2082 | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。免稅適用於生產前環境。 |
| 2082 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 2082 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2082 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2082 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 2082 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 2082 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 2082 | rds-snapshot-encrypted | 確保已針對 Amazon Relationa l Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2082 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2082 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 2082 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2091 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2091 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2091 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2598 | elb-custom-security-policy-ssl-check | 為了協助保護傳輸中的資料，請確定您的傳統 ElasticLoadBalancer SSL 接聽程式使用自訂安全性原則。這些政策可提供各種高強度的密碼編譯演算法，以協助確保系統之間的加密網路通訊。此規則需要您設定自訂的 SSL 接聽程式安全政策。預設的安全政策為：Protocol-TLSv1.2、ECDHE-ECDSA-AES128-GCM-SHA256。 |
| 2600 | elb-custom-security-policy-ssl-check | 為了協助保護傳輸中的資料，請確定您的傳統 ElasticLoadBalancer SSL 接聽程式使用自訂安全性原則。這些政策可提供各種高強度的密碼編譯演算法，以協助確保系統之間的加密網路通訊。此規則需要您設定自訂的 SSL 接聽程式安全政策。預設的安全政策為：Protocol-TLSv1.2、ECDHE-ECDSA-AES128-GCM-SHA256。 |
| 2726 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3021 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 3021 | kms-cmk-for-each-data-classification (製程檢查) | 已針對每個不同的資料分類至少定義一個 KMS 客戶主金鑰 (CMK)，並使用這些 CMK 來加密儲存在該分類中的所有資料。 |
| 3205 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 3449 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3449 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存映像的完整性和安全性新增一層驗證。 |
| 3449 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 3451 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3451 | ec2-關鍵-security-patch-auto-approval（過程檢查） | Patch Manager 中已設定適用於 Windows 及/或 Linux 的修補基準，包括在發佈後 2 天內自動核准重要的安全修補程式。 |
| 3452 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 3452 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 3452 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3453 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 3453 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| 3562 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3562 | cloudfront-associated-with-waf | 此控制項會檢查 CloudFront 發行版是否與 AWS WAF 或 AWS WAFv2 網路 ACL 相關聯。如果分配與 Web ACL 沒有關聯，則控制項會失敗。AWS WAF 是一種 Web 應用程式防火牆，可協助保護 Web 應用程式和 API 免受攻擊。其可讓您設定一組稱為 Web 存取控制清單 (Web ACL) 的規則，該組規則可根據您定義的可自訂 Web 安全規則與條件來允許、封鎖或計數 Web 請求。確保您的 CloudFront 發行版與 AWS WAF Web ACL 相關聯，以協助保護其免受惡意攻擊。您必須在 us-east-1 區域中套用此規則。 |
| 3562 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3562 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3562 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3562 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3562 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 3562 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3562 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 3562 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 3562 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3562 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3562 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3562 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3562 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 3562 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 3562 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 3623 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3623 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 3623 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 3623 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 3815 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 3875 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 3875 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 4333 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4441 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |
| 4441 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 4441 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 4441 | rds-snapshot-encrypted | 確保已針對 Amazon Relationa l Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 4441 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4441 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 4441 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 4445 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4445 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 4829 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 4829 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4829 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) 叢集應啟用多可用區複寫，以利提升已儲存資料的可用性。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 4829 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 4838 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4838 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 4838 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 4838 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4838 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 4839 | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| 4839 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 4839 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4839 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4839 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4839 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 4839 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4839 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4839 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 4839 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4839 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 4839 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4839 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 4839 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4839 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 4839 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 4839 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 4849 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4849 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 4849 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 4849 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 4849 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4849 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 4849 | rds-cluster-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |
| 4849 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 4849 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4849 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 4849 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 6843 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6843 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 6852 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 6852 | federate-with-central-idp (處理程序檢查) | 需要存取 AWS 資源的人力身分識別會使用與 SSO 聯合的中央 IdP 進行驗證。 AWS 中央 IdP 會在 3 次嘗試登入失敗後鎖定系統使用者。 |
| 6860 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6860 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 6861 | cloudtrail-security-trail-enabled | 此規則可檢查啟用多個設定 AWS CloudTrail，以協助確保使用 AWS 建議的安全性最佳作法。其中包括使用記錄加密、記錄驗證，以及 AWS CloudTrail 在多個區域中啟用。 |
| 6953 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6953 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 7436 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 7436 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7436 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 7436 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 7437 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7437 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 7437 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 7437 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7466 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| 7466 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 7466 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制，限制執行個體中繼資料的變更。 |
| 7466 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7466 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 7466 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |
| 7466 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7466 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 7466 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 7466 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7466 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 7466 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 7466 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7466 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 7466 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 7466 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 7466 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |
| 7496 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7496 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 7496 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7496 | cloudfront-accesslogs-enabled | 此控制項會檢查是否已在 CloudFront 分發上啟用伺服器存取記錄。如果未針對分佈啟用存取日誌記錄，則此控制會失敗。CloudFront 訪問日誌提供有關 CloudFront 接收的每個用戶請求的詳細信息。每個日誌都包含收到請求的日期和時間、提出請求的檢視者 IP 地址、請求的來源，以及檢視者提出請求的連接埠號碼等資訊。這些日誌適用於安全與存取稽核及鑑識調查等應用程式。您必須在 us-east-1 區域中套用此規則。 |
| 7496 | cloudwatch-log-group-encrypted | 為協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 7496 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 7496 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 7496 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供有關 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

### 範本

該模板可用於 GitHub：NZISM 的操作最佳實踐。

## PCI DSS 3.2.1 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供支付卡產業資料安全標準 (PCI DSS) 3.2.1 與 AWS 受管 Config 規則之間的對應範例。每個 AWS Config 規則都會套用至特定 AWS 資源，並與一或多個 PCI DSS 控制項相關。一個 PCI DSS 控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
|---|---|---|---|
| | | | 遠端) 流量，有助於限制遠端存取。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.2.1 | 將傳入和傳出流量限制在對於持卡人資料環境必要的流量，並明確拒絕所有其他流量。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3 | 禁止在網際網路與持卡人資料環境中的任何系統元件之間進行直接公開存取。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.1 | 實作 DMZ，將傳入流量僅限於提供經授權可公開存取服務、通訊協定和連接埠的系統元件。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.2 | 將傳入網際網路流量限制在 DMZ 內的 IP 地址。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.4 | 不允許持卡人資料環境有未經授權的傳出流量流向網際網路。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，無需網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | netfw-policy-rule-group-associated | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包與流量流程，並定義預設流量處理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | netfw-stateless-rule-group-not-empty | AWS Network Firewall 規則群組包含定義防火牆如何處理 VPC 中流量的規則。防火牆政策中存在的空白無狀態規則群組不會處理流量。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 1.3.6 | 將存放持卡人資料 (例如資料庫) 的系統元件置放在內部網路區域，並與 DMZ 和其他不受信任的網路隔離。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 2.1 | 一律變更廠商提供的預設值，並在於網路上安裝系統前先移除或停用不必要的預設帳戶。這適用於所有默認密碼，包括但不限於操作系統使用的密碼，提供安全服務的軟件，應用程序和系統帳戶， point-of-sale （POS）終端機，支付應用程序，簡單網絡管理協議（SNMP）社區字符串等）。 | rds-cluster-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Relational Database Service (Amazon RDS) 資料庫叢集的受攻擊面。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1 | 一律變更廠商提供的預設值，並在於網路上安裝系統前先移除或停用不必要的預設帳戶。這適用於所有默認密碼，包括但不限於操作系統使用的密碼，提供安全服務的軟件，應用程序和系統帳戶， point-of-sale （POS）終端機，支付應用程序，簡單網絡管理協議（SNMP）社區字符串等）。 | rds-instance-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體的受攻擊面。 |
| 2.1 | 一律變更廠商提供的預設值，並在於網路上安裝系統前先移除或停用不必要的預設帳戶。這適用於所有默認密碼，包括但不限於操作系統使用的密碼，提供安全服務的軟件，應用程序和系統帳戶， point-of-sale （POS）終端機，支付應用程序，簡單網絡管理協議（SNMP）社區字符串等）。 | redshift-default-admin-check | 由於預設使用者名稱是公開知識，因此變更預設使用者名稱可協助減少 Amazon Redshift 叢集的受攻擊面。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1 | 一律變更廠商提供的預設值，並在於網路上安裝系統前先移除或停用不必要的預設帳戶。這適用於所有默認密碼，包括但不限於操作系統使用的密碼，提供安全服務的軟件，應用程序和系統帳戶， point-of-sale （POS）終端機，支付應用程序，簡單網絡管理協議（SNMP）社區字符串等）。 | redshift-default-db-name-check | 預設名稱是公開知識，應在設定時進行變更。變更 Amazon Redshift 叢集的預設資料庫名稱可協助減少 Redshift 叢集的受攻擊面。 |
| 2.1 | 一律變更廠商提供的預設值，並在於網路上安裝系統前先移除或停用不必要的預設帳戶。這適用於所有默認密碼，包括但不限於操作系統使用的密碼，提供安全服務的軟件，應用程序和系統帳戶， point-of-sale （POS）終端機，支付應用程序，簡單網絡管理協議（SNMP）社區字符串等）。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.1 | 一律變更廠商提供的預設值，並在於網路上安裝系統前先移除或停用不必要的預設帳戶。這適用於所有默認密碼，包括但不限於操作系統使用的密碼，提供安全服務的軟件，應用程序和系統帳戶， point-of-sale （POS）終端機，支付應用程序，簡單網絡管理協議（SNMP）社區字符串等）。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrai l 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | ec2-instance-multiple-eni-check | 此規則會檢查您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體是否擁有多個 ENI。擁有多個 ENI 可能會導致雙主目錄執行個體，也就是具有多個子網路的執行個體。這可能會增加網路安全複雜性，並導致意外的網路路徑和存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準的來源可能包括但不限於：網際網路安全中心 (CIS)「美分國際標準化組織」(ISO)「 SysAdmin 審核網路安全性 (SANS) 研究所」或「美國國家標準技術研究所 (NIST)」。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控庫存清單中未使用的安全群組並管理您的環境。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準的來源可能包括但不限於：網際網路安全中心 (CIS)「美分國際標準化組織」(ISO)「 SysAdmin 審核網路安全性 (SANS) 研究所」或「美國國家標準技術研究所 (NIST)」。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 2.2 | 為所有系統元件制定組態標準。確認這些標準能夠處理所有已知的安全漏洞，並和業界接受的系統強化標準一致。業界公認的系統強化標準來源可能包括但不限於：• 網際網路安全中心 (CIS) • 國際標準化組織 (ISO) • SysAdmin 稽核網路安全性 (SANS) 研究所 • 國家標準技術研究所 (NIST)。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.2.2 | 根據系統功能的要求，僅啟用必要的服務、通訊協定、常駐程式等。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 2.2.3 | 為任何視為不安全的必要服務、通訊協定或常駐程式，實作額外的安全功能。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.3 | 使用強式密碼編譯，加密所有非主控台管理存取。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.3 | 使用強式密碼編譯，加密所有非主控台管理存取。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 2.3 | 使用強式密碼編譯，加密所有非主控台管理存取。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.3 | 使用強式密碼編譯，加密所有非主控台管理存取。 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.3 | 使用強式密碼編譯，加密所有非主控台管理存取。 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 2.4 | 維護位於 PCI DSS 範圍中的系統元件清查。 | ec2-security-group-attached-to-eni-periodic | 此規則可確保安全群組連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 ENI。此規則有助於監控清查中未使用的安全群組並管理您的環境。 |
| 2.4 | 維護位於 PCI DSS 範圍中的系統元件清查。 | eip-attached | 此規則可確保配置給 Amazon Virtual Private Cloud (Amazon VPC) 的彈性 IP 已連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用中的彈性網路介面。此規則有助於監控環境中未使用的 EIP。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 2.4 | 維護位於 PCI DSS 範圍中的系統元件清查。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 2.4 | 維護位於 PCI DSS 範圍中的系統元件清查。 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1 | 針對所有持卡人資料 (CHD) 儲存，至少實作以下資料保留和處置政策、程序及流程，以盡可能儲存最少的持卡人資料：• 將資料儲存量和保留時間限制在符合法律、法規和/或業務要求所需 • 持卡人資料的特定保留要求 • 當資料不再需要時，安全刪除資料的程序 • 每季識別並安全刪除超過定義保留期之儲存持卡人資料的程序。 | s3-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1 | 針對所有持卡人資料 (CHD) 儲存，至少實作以下資料保留和處置政策、程序及流程，以盡可能儲存最少的持卡人資料：• 將資料儲存量和保留時間限制在符合法律、法規和/或業務要求所需 • 持卡人資料的特定保留要求 • 當資料不再需要時，安全刪除資料的程序 • 每季識別並安全刪除超過定義保留期之儲存持卡人資料的程序。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1 | 針對所有持卡人資料 (CHD) 儲存，至少實作以下資料保留和處置政策、程序及流程，以盡可能儲存最少的持卡人資料：• 將資料儲存量和保留時間限制在符合法律、法規和/或業務要求所需 • 持卡人資料的特定保留要求 • 當資料不再需要時，安全刪除資料的程序 • 每季識別並安全刪除超過定義保留期之儲存持卡人資料的程序。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| 3.1 | 針對所有持卡人資料 (CHD) 儲存，至少實作以下資料保留和處置政策、程序及流程，以盡可能儲存最少的持卡人資料：• 將資料儲存量和保留時間限制在符合法律、法規和/或業務要求所需 • 持卡人資料的特定保留要求 • 當資料不再需要時，安全刪除資料的程序 • 每季識別並安全刪除超過定義保留期之儲存持卡人資料的程序。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.4 | 使用以下任一方法，將 PAN 轉譯為在任何一個儲存位置 (包括可攜式數位媒體、備份媒體及日誌) 皆無法讀取的狀態：• 以強式密碼編譯為基礎的單向雜湊 (雜湊必須屬於整個 PAN) • 截斷 (無法使用雜湊來取代截斷的 PAN 區段) • 索引字符和填補 (必須安全地儲存填補) • 強式密碼編譯以及相關聯的金鑰管理流程和程序。注意：如果惡意人士可同時存取 PAN 的截斷和雜湊版本，就能輕而易舉重建原始 PAN 資料。如果實體環境中存在相同 PAN 的雜湊和截斷版本，則必須提供額外的控制措施，以確保無法將雜湊和截斷版本相關聯來重建原始 PAN。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.2 | 限制只有最少的必要保管人才能存取密碼編譯金鑰。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.2 | 限制只有最少的必要保管人才能存取密碼編譯金鑰。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.3 | 始終以下列一種（或多種）形式存儲用於加密/解密持卡人數據的密鑰和私鑰：• 使用至少與數據一樣強度的密鑰加密密鑰加密-加密密鑰，並且與數據加密密鑰分開存儲 • 在安全的加密設備（例如硬件（主機）安全模塊（HSM）中分開存儲 • 在安全的加密設備（例如硬件（主機）安全模塊（HSM）或至少兩個 PTS 批准的 point-of-interaction 設備中按照行業接受的方法進行關鍵股票注意：公鑰不需要將公鑰存儲在其中一個這些形式。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.3 | 始終以下列一種（或多種）形式存儲用於加密/解密持卡人數據的密鑰和私鑰：• 使用至少與數據一樣強度的密鑰加密密鑰加密-加密密鑰，並且與數據加密密鑰分開存儲 • 在安全的加密設備（例如硬件（主機）安全模塊（HSM）中分開存儲 • 在安全的加密設備（例如硬件（主機）安全模塊（HSM）或至少兩個 PTS 批准的 point-of-interaction 設備中按照行業接受的方法進行關鍵股票注意：公鑰不需要將公鑰存儲在其中一個這些形式。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5.3 | 始終以下列一種（或多種）形式存儲用於加密/解密持卡人數據的密鑰和私鑰：• 使用至少與數據一樣強度的密鑰加密密鑰加密-加密密鑰，並且與數據加密密鑰分開存儲 • 在安全的加密設備（例如硬件（主機）安全模塊（HSM）中分開存儲 • 在安全的加密設備（例如硬件（主機）安全模塊（HSM）或至少兩個 PTS 批准的 point-of-interaction 設備中按照行業接受的方法進行關鍵股票注意：公鑰不需要將公鑰存儲在其中一個這些形式。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 3.6.4 | 密碼編譯金鑰會依照相關應用程式廠商或金鑰擁有者的定義，並根據業界最佳實務和指導方針 (例如 NIST 特別出版物 800-57)，在金鑰到達其密碼週期結尾後變更 (例如在定義的時段過後和/或在指定的金鑰產生一定數量的加密文字後)。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.6.5 | 當金鑰的完整性變弱 (例如知道純文字金鑰元件的員工離職) 或金鑰疑似遭到洩漏時，請視需要淘汰或更換 (例如封存、銷毀和/或撤銷) 金鑰。注意：如果需要保留已淘汰或更換的密碼編譯金鑰，則必須安全地封存這些金鑰 (例如透過使用金鑰加密金鑰)。已封存的密碼編譯金鑰只能用於解密/驗證。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 3.6.7 | 防止未經授權替換密碼編譯金鑰。 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.1 | 在透過開放式公有網路傳輸期間，使用強式密碼編譯和安全通訊協定來保護敏感的持卡人資料，包括：• 僅接受信任的金鑰和憑證。• 使用中的通訊協定僅支援安全的版本或組態。• 加密強度適合使用中的加密方法。開放式公有網路範例包括但不限於：• 網際網路 • 無線技術，包括 802.11 和藍牙 • 行動數據技術，例如全球行動通訊系統 (GSM)、分碼多重進接 (CDMA) • 整合封包無線電服務 (GPRS) • 衛星通訊 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 6.2 | 透過安裝由廠商提供的適當安全修補程式，確保所有系統元件和軟體都不受已知漏洞的威脅。在發行後的一個月內安裝重要的安全修補程式。注意：應根據「要求 6.1」中定義的風險排名程序來確定重要的安全修補程式。 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.2 | 透過安裝由廠商提供的適當安全修補程式，確保所有系統元件和軟體都不受已知漏洞的威脅。在發行後的一個月內安裝重要的安全修補程式。注意：應根據「要求 6.1」中定義的風險排名程序來確定重要的安全修補程式。 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 6.2 | 透過安裝由廠商提供的適當安全修補程式，確保所有系統元件和軟體都不受已知漏洞的威脅。在發行後的一個月內安裝重要的安全修補程式。注意：應根據「要求 6.1」中定義的風險排名程序來確定重要的安全修補程式。 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.2 | 透過安裝由廠商提供的適當安全修補程式，確保所有系統元件和軟體都不受已知漏洞的威脅。在發行後的一個月內安裝重要的安全修補程式。注意：應根據「要求 6.1」中定義的風險排名程序來確定重要的安全修補程式。 | ecs-fargate-latest-platform-version | 系統會針對您的 AWS Fargate 工作自動部署安全性更新和修補程式。如果發現影響 AWS Fargate 平台版本的安全性問題，請 AWS 修補平台版本。若要協助對執行 AWS Fargate 的 Amazon 彈性容器服務 (ECS) 任務進行修補程式管理，請更新您的服務獨立任務以使用最新的平台版本。 |
| 6.2 | 透過安裝由廠商提供的適當安全修補程式，確保所有系統元件和軟體都不受已知漏洞的威脅。在發行後的一個月內安裝重要的安全修補程式。注意：應根據「要求 6.1」中定義的風險排名程序來確定重要的安全修補程式。 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.2 | 透過安裝由廠商提供的適當安全修補程式，確保所有系統元件和軟體都不受已知漏洞的威脅。在發行後的一個月內安裝重要的安全修補程式。注意：應根據「要求 6.1」中定義的風險排名程序來確定重要的安全修補程式。 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3.2 | 在發行到生產環境或客戶之前檢閱自訂程式碼，以識別任何潛在的編碼漏洞 (使用手動或自動化程序)，至少包括下列程序：• 由原始程式碼作者以外且熟悉程式碼檢閱技術和安全編碼實務的人士檢閱程式碼變更。• 程式碼檢閱可確保根據安全的編碼指導方針來開發程式碼 • 發行前實作適當的修正。• 管理階層在發行前檢閱並核准程式碼檢閱結果。(續下頁) | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.6 | 對於公開 Web 應用程式，持續解決新的威脅和漏洞，並確保這些應用程式透過下列任一方法防範已知攻擊：• 至少每年並在任何變更之後，透過手動或自動化應用程式漏洞安全評估工具或方法來檢閱公開 Web 應用程式 注意：此評估與針對「要求 11.2」執行的漏洞掃描不同。• 安裝自動化技術解決方案來偵測並防止公開 Web 應用程式前端的 Web 型攻擊 (例如 Web 應用程式防火牆)，以持續檢查所有流量。 | alb-desync-mode-check | 若要協助保護應用程式的 HTTP 去同步漏洞，請確定已在 Application Load Balancer 上啟用 HTTP 去同步緩解模式。HTTP 去同步問題可能會導致請求走私，並使您的應用程式容易遭受請求佇列或快取中毒的危害。去同步緩解模式分為監控、防禦性和最嚴格。預設模式為防禦性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.6 | 對於公開 Web 應用程式，持續解決新的威脅和漏洞，並確保這些應用程式透過下列任一方法防範已知攻擊：• 至少每年並在任何變更之後，透過手動或自動化應用程式漏洞安全評估工具或方法來檢閱公開 Web 應用程式 注意：此評估與針對「要求 11.2」執行的漏洞掃描不同。• 安裝自動化技術解決方案來偵測並防止公開 Web 應用程式前端的 Web 型攻擊 (例如 Web 應用程式防火牆)，以持續檢查所有流量。 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.6 | 對於公開 Web 應用程式，持續解決新的威脅和漏洞，並確保這些應用程式透過下列任一方法防範已知攻擊：• 至少每年並在任何變更之後，透過手動或自動化應用程式漏洞安全評估工具或方法來檢閱公開 Web 應用程式 注意：此評估與針對「要求 11.2」執行的漏洞掃描不同。• 安裝自動化技術解決方案來偵測並防止公開 Web 應用程式前端的 Web 型攻擊 (例如 Web 應用程式防火牆)，以持續檢查所有流量。 | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.6 | 對於公開 Web 應用程式，持續解決新的威脅和漏洞，並確保這些應用程式透過下列任一方法防範已知攻擊：• 至少每年並在任何變更之後，透過手動或自動化應用程式漏洞安全評估工具或方法來檢閱公開 Web 應用程式 注意：此評估與針對「要求 11.2」執行的漏洞掃描不同。• 安裝自動化技術解決方案來偵測並防止公開 Web 應用程式前端的 Web 型攻擊 (例如 Web 應用程式防火牆)，以持續檢查所有流量。 | waf-regional-rule-not-empty | 確保 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.6 | 對於公開 Web 應用程式，持續解決新的威脅和漏洞，並確保這些應用程式透過下列任一方法防範已知攻擊：• 至少每年並在任何變更之後，透過手動或自動化應用程式漏洞安全評估工具或方法來檢閱公開 Web 應用程式 注意：此評估與針對「要求 11.2」執行的漏洞掃描不同。• 安裝自動化技術解決方案來偵測並防止公開 Web 應用程式前端的 Web 型攻擊 (例如 Web 應用程式防火牆)，以持續檢查所有流量。 | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.6 | 對於公開 Web 應用程式，持續解決新的威脅和漏洞，並確保這些應用程式透過下列任一方法防範已知攻擊：• 至少每年並在任何變更之後，透過手動或自動化應用程式漏洞安全評估工具或方法來檢閱公開 Web 應用程式 注意：此評估與針對「要求 11.2」執行的漏洞掃描不同。• 安裝自動化技術解決方案來偵測並防止公開 Web 應用程式前端的 Web 型攻擊 (例如 Web 應用程式防火牆)，以持續檢查所有流量。 | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 7.1.1 | 定義每個角色的存取需求，包括：• 每個角色針對其工作職能所需存取的系統元件和資料資源 • 存取資源所需的權限等級 (例如使用者、管理員等)。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 7.1.2 | 將特殊權限使用者 ID 的存取限制在執行工作職責所需的最低權限。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 7.2.1 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：所有系統元件的涵蓋範圍 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | ecs-containers-nonprivileged | 若要協助實作最低權限原則，則 Amazon Elastic Container Service (Amazon ECS) 任務定義不應啟用提升的權限。當此參數為 true 時，容器在主機容器執行個體上會有更高的權限 (類似超級使用者)。 |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | ecs-containers-readonly-access | 啟用 Amazon Elastic Container Service (ECS) 容器的唯讀存取權，可協助遵守最低權限原則。此選項可以減少攻擊媒介，因為除非具有明確的讀寫許可，否則無法修改容器執行個體的檔案系統。 |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權合併，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 7.2.2 | 為系統元件建立存取控制系統，根據使用者需要知道的內容限制存取，並且除非明確允許，否則「拒絕所有」其他存取。此存取控制系統必須包含以下內容：根據工作分類和職能將權限指派給個人。 | opensearch-access-control-enabled | 確保在您的 Amazon OpenSearch 服務網域上啟用了精細的存取控制。精細的存取控制提供增強的授權機制，以實現對 Amazon Ser OpenSearch vice 網域的最低權限存取。它允許以角色為基礎的網域存取控制，以及索引、文件和欄位層級安全性、多租戶 OpenSearch 服務儀表板支援，以及適用於服務和 Kibana 的 HTTP 基本驗證。OpenSearch |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 7.2.3 | 預設「全部拒絕」設定。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 8.1.1 | 在允許使用者存取系統元件或持卡人資料之前，為所有使用者指派唯一 ID。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1.4 | 在 90 天內移除/停用非作用中的使用者帳戶。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | codebuild-project-environment-privileged-check | 為了協助實施最低特權原則，請確保您的 Amazon CodeBuild 專案環境未啟用特權模式。您應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | ecs-no-environment-secrets | 安全最佳實務是將敏感資訊傳遞給容器做為環境變數。您可以在 Amazon ECS 任務定義的容器定義中參照儲存在 AWS 系統管理員參數存放區或機 AWS Secrets Manager 管理員中的值，將資料安全地插入 Amazon 彈性容器服務 (ECS) 容器。然後，您可以公開做為環境變數或位於容器日誌組態中的敏感資訊。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch務) 網域已啟用加密。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relationa l Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 8.2.1 | 在傳輸期間和在所有系統元件上儲存的期間，使用強式密碼編譯將所有驗證憑證 (例如密碼/複雜密碼) 轉譯為無法讀取的狀態。 | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.3 | 密碼/複雜密碼必須符合下列條件：• 長度下限必須至少為七個字元。• 同時包含數字和字母字元。或者，密碼/複雜密碼必須具有至少相當於以上指定參數的複雜性和強度。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則允許您選擇性地設定 RequireUppercaseCharacters (PCI DSS 預設值：假)、 RequireLowercaseCharacters (PCI DSS 預設值：真)、 RequireSymbols (PCI DSS 預設值：假)、 RequireNumbers (PCI DSS 預設值：真)、 MinimumPasswordLength (PCI DSS 預設值：7)、 (PCI DSS 預設值：4)，以及 PasswordReusePrevention MaxPasswordAge (PCI DSS 預設值：90) 為您的 IAM 密碼政策。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.4 | 至少每 90 天更改一次用戶密碼/密碼。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.4 | 至少每 90 天更改一次用戶密碼/密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則允許您選擇性地設定 RequireUppercaseCharacters (PCI DSS 預設值：假)、 RequireLowercaseCharacters (PCI DSS 預設值：真)、 RequireSymbols (PCI DSS 預設值：假)、 RequireNumbers (PCI DSS 預設值：真)、 MinimumPasswordLength (PCI DSS 預設值：7)、 (PCI DSS 預設值：4)，以及 PasswordReusePrevention MaxPasswordAge (PCI DSS 預設值：90) 為您的 IAM 密碼政策。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.4 | 至少每 90 天更改一次用戶密碼/密碼。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.2.5 | 不允許個人提交與最近所使用四個密碼/複雜密碼中任何一個相同的新密碼/複雜密碼。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則允許您選擇性地設定 RequireUppercaseCharacters (PCI DSS 預設值：假)、 RequireLowercaseCharacters (PCI DSS 預設值：真)、 RequireSymbols (PCI DSS 預設值：假)、 RequireNumbers (PCI DSS 預設值：真)、 MinimumPasswordLength (PCI DSS 預設值：7)、 (PCI DSS 預設值：4)，以及 PasswordReusePrevention MaxPasswordAge (PCI DSS 預設值：90) 為您的 IAM 密碼政策。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.3.1 | 為具有管理存取權限的人員對 CDE 的所有非主控台存取，整合多重要素驗證。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| 8.3.1 | 為具有管理存取權限的人員對 CDE 的所有非主控台存取，整合多重要素驗證。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.3.1 | 為具有管理存取權限的人員對 CDE 的所有非主控台存取，整合多重要素驗證。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 8.3.1 | 為具有管理存取權限的人員對 CDE 的所有非主控台存取，整合多重要素驗證。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.3.2 | 為來自外部實體網路的所有遠端網路存取 (使用者和管理員，並包括為了支援或維護的第三方存取)，整合多重要素驗證。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA 可減少帳戶遭到入侵的事件。 |
| 8.3.2 | 為來自外部實體網路的所有遠端網路存取 (使用者和管理員，並包括為了支援或維護的第三方存取)，整合多重要素驗證。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在使用者名稱和密碼之外，多增加一層保護。要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.3.2 | 為來自外部實體網路的所有遠端網路存取 (使用者和管理員，並包括為了支援或維護的第三方存取)，整合多重要素驗證。 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 8.3.2 | 為來自外部實體網路的所有遠端網路存取 (使用者和管理員，並包括為了支援或維護的第三方存取)，整合多重要素驗證。 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為使用者名稱和密碼多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.1 | 實作稽核記錄，將所有對系統元件的存取連結到每個個別使用者。 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.1 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：所有個別使用者對持卡人資料的存取 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.2 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：具備根或管理權限之個別使用者所採取的所有動作 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.3 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：存取所有稽核記錄 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.4 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：邏輯存取嘗試無效 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.5 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：使用和變更識別與驗證機制 (包括但不限於建立新帳戶和提升權限)，以及對具有根或管理權限之帳戶進行的所有變更、新增或刪除 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.6 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：初始化、停止或暫停稽核日誌 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 10.2.6 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：初始化、停止或暫停稽核日誌 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.6 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：初始化、停止或暫停稽核日誌 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 10.2.7 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：建立和刪除系統層級物件 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.7 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：建立和刪除系統層級物件 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 10.2.7 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：建立和刪除系統層級物件 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.7 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：建立和刪除系統層級物件 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 10.2.7 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：建立和刪除系統層級物件 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 10.2.7 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：建立和刪除系統層級物件 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.2.7 | 實作所有系統元件的自動化稽核記錄，以重建下列事件：建立和刪除系統層級物件 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌提供有關建置專案的詳細資訊。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.3.1 | 為每個事件的所有系統元件記錄至少下列的稽核記錄項目：使用者識別 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| 10.5 | 保護稽核記錄以免遭到更改。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.5 | 保護稽核記錄以免遭到更改。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 10.5 | 保護稽核記錄以免遭到更改。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.5.2 | 保護稽核記錄檔案不受未經授權的修改。 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.5.2 | 保護稽核記錄檔案不受未經授權的修改。 | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 10.5.2 | 保護稽核記錄檔案不受未經授權的修改。 | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 10.5.3 | 迅速將稽核記錄檔案備份到難以更改的集中式日誌伺服器或媒體。 | s3-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.5.3 | 迅速將稽核記錄檔案備份到難以更改的集中式日誌伺服器或媒體。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| 10.5.3 | 迅速將稽核記錄檔案備份到難以更改的集中式日誌伺服器或媒體。 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.5.3 | 迅速將稽核記錄檔案備份到難以更改的集中式日誌伺服器或媒體。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動進行物件的非同步複製，以協助確保維護資料可用性。 |
| 10.5.5 | 在日誌上使用檔案完整性監控或變更偵測軟體，確保必須產生提醒，才能變更現有的日誌資料 (但新增資料不應引發提醒)。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.5.5 | 在日誌上使用檔案完整性監控或變更偵測軟體，確保必須產生提醒，才能變更現有的日誌資料 (但新增資料不應引發提醒)。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 10.7 | 保留稽核記錄的歷史記錄至少一年，其中至少三個月可立即進行分析 (例如線上、封存或可從備份還原)。 | s3-lifecycle-policy-check | 請確保設定 Amazon S3 生命週期政策，以協助定義要讓 Amazon S3 在物件生命週期內採取的動作 (例如，將物件轉移至另一個儲存類別、封存物件，或在指定期限後刪除物件)。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 10.7 | 保留稽核記錄的歷史記錄至少一年，其中至少三個月可立即進行分析 (例如線上、封存或可從備份還原)。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| 11.2.3 | 執行內部和外部掃描，並在任何重大變更後視需要重新掃描。掃描必須由合格的人員執行。 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) 映像掃描功能有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上啟用映像掃描功能，可為儲存影像的完整性和安全性新增一層驗證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.4 | 使用入侵偵測和/或入侵預防技術來偵測和/或預防網路入侵。監控持卡人資料環境周邊以及持卡人資料環境中關鍵點的所有流量，並提醒人員可疑的入侵。將所有入侵偵測和預防引擎、基準和簽章保持在最新狀態。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 11.4 | 使用入侵偵測和/或入侵預防技術來偵測和/或預防網路入侵。監控持卡人資料環境周邊以及持卡人資料環境中關鍵點的所有流量，並提醒人員可疑的入侵。將所有入侵偵測和預防引擎、基準和簽章保持在最新狀態。 | netfw-policy-rule-group-associated | AWS Network Firewall 政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包與流量流程，並定義預設流量處理。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.5 | 部署變更偵測機制 (例如檔案完整性監控工具)，提醒人員對關鍵系統檔案、組態檔案或內容檔案的未經授權修改 (包括變更、新增和刪除)；並設定軟體，每週至少執行一次關鍵檔案的比較。 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 11.5 | 部署變更偵測機制 (例如檔案完整性監控工具)，提醒人員對關鍵系統檔案、組態檔案或內容檔案的未經授權修改 (包括變更、新增和刪除)；並設定軟體，每週至少執行一次關鍵檔案的比較。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

### 範本

此範本可在下列網站取得 GitHub：PCI DSS 3.2.1 的營運最佳作法。

## 可公開存取資源的操作最佳實務

此一致性套件有助於識別可公開存取的資源。

如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：可公開存取資源的營運最佳實務。

# RBI 城市合作銀行 (UCB) 網路安全架構的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了印度儲備銀行（RBI）城市合作銀行網絡安全框架（UCBS）和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則適用於特定 AWS 資源，並與 UCBS 控件的一個或多個 RBI 網絡安全框架相關。一個 RBI 城市合作銀行 (UCB) 網路安全架構控制可以與多個 Config 規則相關聯。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.1) | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| Annex_I(1.1) | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| Annex_I(1.1) | ecr-private-tag-immutability-enabled | 啟用 Elastic Container Repository (ECR) 標籤不變性，防止 ECR 映像上的映像標籤遭到覆寫。先前標籤可能會 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 遭到覆蓋，並需要手動方法來唯一識別映像。 |
| Annex_I(1.3) | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| Annex_I(1.3) | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Annex_I(1.3) | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Annex_I(1.3) | api-gw-cache-enabled-and-encrypted | 為了協助保護靜態資料，請確保已針對 API Gateway 階段的快取啟用加密功能。由於可以針對 API 方法擷取敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Annex_I(1.3) | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| Annex_I(1.3) | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Annex_I(1.3) | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Annex_I(1.3) | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| Annex_I(1.3) | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| Annex_I(1.3) | backup-recovery-point-encrypted | 確定已啟用 AWS Backup 復原點的加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | codebuild-project-artifact-encryption | 若要協助保護靜態敏感資料，請確定已為 AWS CodeBuild 成品啟用加密功能。 |
| Annex_I(1.3) | codebuild-project-s3-logs-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon S3 中存放的 AWS CodeBuild 日誌啟用加密。 |
| Annex_I(1.3) | opensearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon Ser OpenSearch vice 網域已啟用加密。 |
| Annex_I(1.3) | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| Annex_I(1.3) | opensearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | dynamodb-table-encrypted-kms | 確保已針對 Amazon DynamoDB 資料表啟用加密功能。由於這些資料表中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。根據預設，DynamoDB 表格會使用 AWS 擁有的客戶主金鑰 (CMK) 加密。 |
| Annex_I(1.3) | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Annex_I(1.3) | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| Annex_I(1.3) | elasticsearch-encrypted-at-rest | 由於敏感資料可以存在並協助保護靜態資料，因此請確保您的 Amazon OpenSearch 服務 (服OpenSearch 務) 網域已啟用加密。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | elasticsearch-node-to-node-encryption-check | 確保已啟用 Amazon OpenSearch 服務的 node-to-node 加密。N ode-to-node 加密可為 Amazon Virtual Private Cloud (Amazon VPC) 內的所有通訊啟用 TLS 1.2 加密。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Annex_I(1.3) | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| Annex_I(1.3) | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Annex_I(1.3) | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| Annex_I(1.3) | rds-snapshot-encrypted | 確保已針對 Amazon Relational Database Service (Amazon RDS) 快照啟用加密功能。由於可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Annex_I(1.3) | rds-storage-encrypted | 為了協助保護靜態資料，請確保已針對 Amazon Relational Database Service (Amazon RDS) 執行個體啟用加密功能。由於 Amazon RDS 執行個體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Annex_I(1.3) | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| Annex_I(1.3) | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| Annex_I(1.3) | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | sagemaker-endpoint-configuration-kms-key-configured | 為了協助保護靜態資料，請確保您的 SageMaker 端點已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 端點中，因此請啟用靜態加密以協助保護該資料。 |
| Annex_I(1.3) | sagemaker-notebook-instance-kms-key-configured | 為了協助保護靜態資料，請確定您的 SageMaker 筆記型電腦已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於機密資料可能存在於 SageMaker 筆記型電腦中，因此請啟用靜態加密以協助保護資料。 |
| Annex_I(1.3) | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Annex_I(1.3) | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| Annex_I(1.3) | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| Annex_I(1.3) | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| Annex_I(1.3) | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| Annex_I(1.3) | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| Annex_I(1.3) | no-unrestricted-route-to-igw | 確保 Amazon EC2 路由表沒有指向網際網路閘道的無限制路由。移除或限制 Amazon VPC 內工作負載對網際網路的存取，可減少環境中的意外存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | redshift-cluster-kms-enabled | 為了協助保護靜態資料，請確保您的 Amazon Redshift 叢集已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Redshift 叢集中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| Annex_I(1.3) | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| Annex_I(1.3) | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |
| Annex_I(1.3) | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。 AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| Annex_I(1.3) | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| Annex_I(1.3) | rds-instance-public-access-check | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |
| Annex_I(1.3) | rds-snapshots-public-prohibited | 確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，以管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| Annex_I(1.3) | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| Annex_I(1.3) | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| Annex_I(1.3) | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| Annex_I(1.3) | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(1.3) | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記型電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| Annex_I(5.1) | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或在環境中耗用過多資源。 |
| Annex_I(5.1) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| Annex_I(5.1) | waf-regional-rule-not-empty | 確保您的 AWS WAF 的規則不是空的。沒有條件的規則可能會導致非預期的行為。 |
| Annex_I(5.1) | waf-regional-rulegroup-not-empty | 確定 AWS WAF 的規則群組不是空的。空白規則群組可能會導致非預期的行為。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(5.1) | waf-regional-webacl-not-empty | 連接至 AWS WAF 的 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 要求。如果 Web ACL 為空白，Web 流量會在不被 WAF 所偵測或採取行動的情況下通過。 |
| Annex_I(5.1) | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| Annex_I(5.1) | api-gw-associated-with-waf | AWS WAF 可讓您設定一組規則 (稱為 Web 存取控制清單 (Web ACL))，以根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 要求。確保您的 Amazon API Gateway 階段與 WAF Web ACL 相關聯，以保護其免於遭受惡意攻擊 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(5.1) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| Annex_I(5.1) | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| Annex_I(6) | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(6) | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| Annex_I(6) | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| Annex_I(6) | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統的最佳實務。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(6) | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |
| Annex_I(6) | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automatedSnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |
| Annex_I(6) | vuln-management-plan-exists（過程檢查） | 確保已制定並實作漏洞管理計畫，以便擁有正式定義的程序來解決環境中的漏洞。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.1) | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」:「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Annex_I(7.1) | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| Annex_I(7.1) | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |
| Annex_I(7.1) | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.1) | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制對系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |
| Annex_I(7.2) | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.3) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| Annex_I(7.4) | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| Annex_I(7.4) | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |
| Annex_I(7.4) | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| Annex_I(7.4) | cloudtrail-s3-dataevents-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.4) | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| Annex_I(7.4) | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| Annex_I(7.4) | cw-loggroup-retention-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.4) | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |
| Annex_I(7.4) | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| Annex_I(7.4) | opensearch-audit-logging-enabled | 確保您的 Amazon OpenSearch 服務網域上已啟用稽核記錄。稽核記錄可讓您追蹤 OpenSearch 網域上的使用者活動，包括驗證成功與失敗、要 OpenSearch求、索引變更以及傳入的搜尋查詢。 |
| Annex_I(7.4) | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.4) | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |
| Annex_I(7.4) | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| Annex_I(7.4) | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relational Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.4) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| Annex_I(7.4) | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| Annex_I(7.4) | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。 AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(7.4) | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDbEncrypted （Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |
| Annex_I(10.2) | security-awareness-program-exists （過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |
| Annex_I(12) | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定保留期，以符合您的恢復能力要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(12) | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| Annex_I(12) | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它還可以透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| Annex_I(12) | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| Annex_I(12) | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(12) | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| Annex_I(12) | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |
| Annex_I(12) | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(12) | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| Annex_I(12) | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| Annex_I(12) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| Annex_I(12) | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |

### 範本

該模板可用於 GitHub：RBI 網絡安全框架的操作最佳實踐 UC BS。

## RBI MD-ITF 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

以下提供了印度儲備銀行（RBI）主要方向-信息技術框架和 AWS 託管 Config 規則之間的示例映射。每個 Config 規則適用於特定 AWS 資源，並與一個或多個 RBI 主要方向-信息技術框架控件相關。一個 RBI 主要指引 – 資訊技術架構控制可以與多個 Config 規則相關。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(a) | 資訊資產的識別和分類。 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| | | | 織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 3.1(a) | 資訊資產的識別和分類。 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |
| 3.1(a) | 資訊資產的識別和分類。 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(a) | 資訊資產的識別和分類。 | ecr-private-tag-immutability-enabled | 啟用 Elastic Container Repository (ECR) 標籤不變性，防止 ECR 映像上的映像標籤遭到覆寫。先前標籤可能會遭到覆寫，並需要使用手動方法來唯一識別映像。 |
| 3.1(c ) | 角色型存取控制 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 3.1(c ) | 角色型存取控制 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 3.1(c ) | 角色型存取控制 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |
| 3.1(c ) | 角色型存取控制 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1(c ) | 角色型存取控制 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 3.1(c ) | 角色型存取控制 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 3.1(c ) | 角色型存取控制 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 3.1(c ) | 角色型存取控制 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 3.1(c ) | 角色型存取控制 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 3.1(c ) | 角色型存取控制 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(c ) | 角色型存取控制 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 3.1(c ) | 角色型存取控制 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 3.1(c ) | 角色型存取控制 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(g) | 事件管理 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 3.1(g) | 事件管理 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(g) | 事件管理 | alb-waf-enabled | 確保在彈性負載平衡器 (ELB) 上啟用 AWS WAF，以協助保護 Web 應用程式。WAF 有助於保護 Web 應用程式或 API 免於常見的網路攻擊。這些網路惡意探索攻擊可能會影響可用性、危及安全性，或耗用過多環境中的資源。 |
| 3.1(g) | 事件管理 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(g) | 事件管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 3.1(h) | 線索 | api-gw-execution-logging-enabled | API Gateway 日誌記錄會顯示存取 API 的使用者及其存取 API 方式的詳細檢視。此洞察功能可讓您掌握使用者活動。 |
| 3.1(h) | 線索 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(h) | 線索 | codebuild-project-logging-enabled | 確保已啟用 AWS CodeBuild 專案記錄，以便將您的建置輸出日誌傳送到 Amazon CloudWatch 或 Amazon Simple Storage Service (Amazon S3)。建置輸出日誌會提供有關建置專案的詳細資訊。 |
| 3.1(h) | 線索 | opensearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。OpenSearch 服務錯誤記錄可協助進行安全性和存取稽核，並可協助診斷可用性問題。 |
| 3.1(h) | 線索 | redshift-audit-logging-enabled | 若要擷取 Amazon Redshift 叢集上的連線和使用者活動相關資訊，請確保已啟用稽核日誌記錄。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(h) | 線索 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 3.1(h) | 線索 | cloudtrail-s3-data events-enabled | 收集 Simple Storage Service (Amazon S3) 資料事件有助於偵測任何異常活動。詳細資 AWS 帳戶 訊包括存取 Amazon S3 儲存貯體的資訊、IP 地址和事件時間。 |
| 3.1(h) | 線索 | cw-loggroup-retent ion-period-check | 確保為日誌群組保留最短的事件日誌資料持續時間，以利故障診斷和鑑識調查。如果缺少可用的過去事件日誌資料，就很難重建和識別潛在的惡意事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(h) | 線索 | elasticsearch-logs-to-cloudwatch | 確保 Amazon OpenSearch 服務網域已啟用錯誤日誌，並將其串流至 Amazon CloudWatch 日誌以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。 |
| 3.1(h) | 線索 | elb-logging-enabled | Elastic Load Balancing 活動是環境內的通訊中心點。請確保已啟用 ELB 日誌記錄。收集的資料可提供有關傳送至 ELB 之請求的詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(h) | 線索 | multi-region-cloudtrail-enabled | AWS CloudTrail 記錄 AWS 管理主控台動作和 API 呼叫。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。 CloudTrail 如果啟用多重 _ AWS 區域，則會將日誌檔案從所有區域傳遞至您的 S3 儲存貯體。此外，當 AWS 啟動新區域時， CloudTrail 將在新區域中建立相同的軌跡。而您會收到包含新區域 API 活動的日誌檔，卻無需採取任何動作。 |
| 3.1(h) | 線索 | rds-logging-enabled | 若要協助您在環境內進行日誌記錄和監控，請確定已啟用 Amazon Relationa l Database Service (Amazon RDS) 日誌記錄。藉由 Amazon RDS 日誌記錄，您可以擷取連線、中斷連線、查詢或查詢的資料表等事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(h) | 線索 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 3.1(h) | 線索 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和協定。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(h) | 線索 | wafv2-logging-enabled | 若要協助您在環境中進行記錄和監控，請在地區和全球 Web ACL 上啟用 AWS WAF (V2) 記錄。AWS WAF 記錄會提供 Web ACL 分析之流量的詳細資訊。記錄會記錄 AWS WAF 從您的 AWS 資源接收要求的時間、請求的相關資訊，以及每個要求相符之規則的動作。 |
| 3.1(h) | 線索 | redshift-cluster-configuration-check | 為了保護靜態資料，請確保已針對 Amazon Redshift 叢集啟用加密功能。您還必須確保已在 Amazon Redshift 叢集上部署必要的組態。應啟用稽核日誌記錄，以提供資料庫中連線和使用者活動的相關資訊。此規則要求為 clusterDb Encrypted（Config 默認值：TRUE）和 loggingEnabled（Config 默認值：TRUE）設置一個值。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(i) | 公有金鑰基礎設施 | acm-certificate-expiration-check | 確保 AWS ACM 頒發 X509 憑證，以確保網路完整性受到保護。這些憑證必須有效且未過期。此規則需要值 daysToExpiration (AWS 基礎安全性最佳作法值：90)。實際值應反映貴組織的政策。 |
| 3.1(i) | 公有金鑰基礎設施 | alb-http-drop-invalid-header-enabled | 確保 Elastic Load Balancer (ELB) 設定為捨棄 http 標頭。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1(i) | 公有金鑰基礎設施 | alb-http-to-https-redirection-check | 為了協助保護傳輸中的資料，請確保 Application Load Balancer 會自動將未加密的 HTTP 請求重新導向至 HTTPS。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(i) | 公有金鑰基礎設施 | api-gw-ssl-enabled | 確保 Amazon API Gateway REST API 階段已使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的請求。 |
| 3.1(i) | 公有金鑰基礎設施 | opensearch-https-required | 由於敏感資料可以存在並協助保護傳輸中的資料，因此請確保啟用 HTTPS 以連線至 Amazon OpenSearch 服務網域。 |
| 3.1(i) | 公有金鑰基礎設施 | elbv2-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(i) | 公有金鑰基礎設施 | elb-acm-certificate-required | 由於可能存在敏感資料並為了協助保護傳輸中資料，因此請確保您的 Elastic Load Balancing 已啟用加密功能。使用 Cer AWS tificate Manager 來管理、佈建和部署包含 AWS 服務和內部資源的公有和私有 SSL/TLS 憑證。 |
| 3.1(i) | 公有金鑰基礎設施 | elb-tls-https-listeners-only | 確保 Elastic Load Balancer (ELB) 已設定使用 SSL 或 HTTPS 接聽程式。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.1(i) | 公有金鑰基礎設施 | redshift-require-tls-ssl | 確保 Amazon Redshift 叢集需要 TLS/SSL 加密才能連線到 SQL 用戶端。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.1(i) | 公有金鑰基礎設施 | s3-bucket-ssl-requests-only | 為協助保護傳輸中的資料，請確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體要求使用 Secure Socket Layer (SSL)。由於可能存在敏感資料，因此請啟用傳輸中加密以協助保護該資料。 |
| 3.3 | 漏洞管理 | elastic-beanstalk-managed-updates-enabled | 針對 Amazon Elastic Beanstalk 環境啟用受管平台更新，可確保已安裝適用於環境的最新可用平台修正、更新和功能。安裝最新的修補程式是保護系統安全的最佳實務。 |
| 3.3 | 漏洞管理 | rds-automatic-minor-version-upgrade-enabled | 在 Amazon Relational Database Service (RDS) 執行個體上啟用自動次要版本升級，以確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新，其中可能包括安全修補程式和錯誤修正。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 漏洞管理 | redshift-cluster-maintenancesettings-check | 此規則可確保 Amazon Redshift 叢集使用貴組織的偏好設定。具體而言，即具有資料庫偏好的維護時段和自動快照保留期。此規則需要您設定 allowVersionUpgrade。預設值為 true。它也可讓您選擇性地設定 preferredMaintenanceWindow (預設值為「星期六:16:00-星期六:16:30」) 和「 automated SnapshotRetention期間」(預設值為 1)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 漏洞管理 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 3.3 | 漏洞管理 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.3 | 漏洞管理 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |
| 3.3 | 漏洞管理 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5 | 網路危機管理計畫 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 3.5 | 網路危機管理計畫 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5 | 網路危機管理計畫 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 3.5 | 網路危機管理計畫 | ec2-managedinstance-association-compliance-status-check | 使用 AWS Systems Manager 關聯來協助清查組織內的軟體平台和應用程式。 AWS Systems Manager 會為您的代管執行個體指派組態狀態，並可讓您設定作業系統修補程式等級、軟體安裝、應用程式組態，以及環境的其他詳細資料的基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 3.5 | 網路危機管理計畫 | ec2-managedinstance-patch-compliance-status-check | 啟用此規則可協助識別和記載 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。該規則會根據組織政策和程序的要求，檢查 AWS Systems Manager 中的 Amazon EC2 執行個體是否符合修補程式合規性。 |
| 3.9 | IT 風險評估 | annual-risk-assessment-performed（過程檢查） | 對貴組織執行年度風險評估。風險評估可協助確定已識別風險和/或漏洞影響組織的可能性及影響內容。 |
| 3.12 | 培訓 | security-awareness-program-exists（過程檢查） | 為貴組織建立並維護安全意識計劃。安全意識計劃可教育員工如何保護其組織免於遭受各種安全缺口或事件侵害。 |
| 4.4(g) | 詐騙分析 - 可疑交易分析、侵占、盜竊或疑似洗錢、挪用資產、操控財務記錄等。向 RBI 報告詐騙行為的監管要求應由系統驅動。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | clb-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | lambda-vpc-multi-az-check | 如果您的 AWS Lambda 函數設定為連線到帳戶中的虛擬私有雲 (VPC)，請在至少兩個不同的可用區域中部署 AWS Lambda 函數，以確保在單一區域中發生服務中斷時，它是您的函數可用來處理事件。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | s3-bucket-default-lock-enabled | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體預設已啟用鎖定。由於 S3 儲存貯體中可能存在靜態敏感資料，因此請強制執行靜態物件鎖定以協助保護該資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | lambda-dlq-check | 啟用此規則可在函數失敗時，透過 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知適當的人員。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk 增強型健康狀態報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 4.4(h) | IT 安全系統的容量和效能分析。 | ebs-optimized-instance | Amazon Elastic Block Store (Amazon EBS) 中的最佳化執行個體可為 Amazon EBS I/O 作業提供額外的專用容量。此最佳化會將 Amazon EBS I/O 操作與執行個體中其他流量之間的爭用降至最低，為 EBS 磁碟區提供最有效率的效能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(h) | IT 安全系統的容量和效能分析。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 4.4(i) | 事件報告、其影響，以及為防止今後再次發生此類事件而採取的步驟。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 4.4(i) | 事件報告、其影響，以及為防止今後再次發生此類事件而採取的步驟。 | guardduty-non-archived-findings | Amazon GuardDuty 透過將發現結果按嚴重性 (低、中和高) 分類，協助您瞭解事件的影響。您可以使用這些分類決定修復策略和優先順序。此規則可讓您根據 Config 織原則的 daysLowSev 要求， daysMediumSev 選擇性地為未存檔的發現項目設定 daysHighSev (組 Config 預設值：30)、(組態預設值：7) 及 (組態預設值：1)。 |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | aurora-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Aurora 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | cmk-backing-key-rotation-enabled | 啟用金鑰輪換功能，以確保金鑰在金鑰到達加密期間結束後進行輪換。 |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | ec2-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Compute Cloud (Amazon EC2) 資源是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | fsx-resources-protected-by-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon FSx 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 6.3 | NBFC 應考慮是否需要為其關鍵業務系統和資料中心設置必要的備份網站。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | dynamodb-autoscaling-enabled | Amazon DynamoDB 自動擴展使用應用 Ap AWS plication Auto Scaling 服務調整佈建的輸送量容量，以自動回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取/寫入容量，不需限流即可處理突然增加的流量。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | elb-cross-zone-load-balancing-enabled | 為 Elastic Load Balancer (ELB) 啟用跨區域負載平衡，以利維持足夠的容量和可用性。跨區域負載平衡可減少在每個啟用的可用區域中維護同等數量執行個體的需求。還可以改善應用程式的能力，以處理一或多個執行個體遺失的狀況。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | elb-deletion-protection-enabled | 此規則可確保 Elastic Load Balancing 已啟用刪除保護。使用此功能可防止意外或惡意刪除負載平衡器，從而導致應用程式喪失可用性。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | clb-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | elbv2-multiple-az | Elastic Load Balancing (ELB) 會自動將傳入流量分配至可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。為了確保高可用性，請確保您的 ELB 已註冊來自多個可用區域的執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | lambda-vpc-multi-az-check | 如果您的 AWS Lambda 函數設定為連線到帳戶中的虛擬私有雲 (VPC)，請在至少兩個不同的可用區域中部署 AWS Lambda 函數，以確保在單一區域中發生服務中斷時，它是您的函數可用來處理事件。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | rds-instance-deletion-protection-enabled | 確保 Amazon Relational Database Service (Amazon RDS) 執行個體已啟用刪除保護。使用刪除保護可防止意外或惡意刪除 Amazon RDS 執行個體，從而導致應用程式喪失可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | rds-multi-az-support | Amazon Relational Database Service (Amazon RDS) 中的多可用區域支援可為資料庫執行個體提供增強的可用性與持久性。佈建多可用區域資料庫執行個體時，Amazon RDS 會自動建立主要資料庫執行個體，並將資料同步複寫到不同可用區域中的待命執行個體。每個可用區域都在其本身不同的實體獨立基礎設施上執行，而且具備高度可靠的設計。如果基礎設施失敗，Amazon RDS 會執行自動容錯移轉到待命執行個體，以便您可以在容錯移轉完成後立即恢復資料庫操作。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | vpc-vpn-2-tunnels-up | 您可以實作備援的站台對站台 VPN 通道以達到恢復能力要求。這會使用兩個通道來確保連線能力，以防其中一個站台對站台 VPN 連線無法使用。為免在無法使用客戶閘道時失去連線，您可以使用第二個客戶閘道設定 Amazon Virtual Private Cloud (Amazon VPC) 和虛擬私有閘道的第二個站台對站台 VPN 連線。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | autoscaling-group-elb-healthcheck-required | Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 群組的 Elastic Load Balancer (ELB) 運作狀態檢查可讓您維持足夠的容量和可用性。負載平衡器會定期傳送 ping、嘗試連線或傳送請求，以測試 Auto Scaling 群組中的 Amazon EC2 執行個體運作狀態。如果執行個體未回報，流量就會傳送到新的 Amazon EC2 執行個體。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | dynamodb-throughput-limit-check | 啟用此規則可確保檢查 Amazon DynamoDB 資料表上的佈建輸送容量。這是每份資料表能夠支援的讀取/寫入活動量。DynamoDB 會使用這項資訊保留足夠的系統資源，以便符合您的輸送量要求。當輸送量接近客戶帳戶的上限時，此規則會產生提醒。此規則可讓您選擇性地設定帳戶管理系統 ThresholdPercentage (組 Config 預設值：80) 與帳戶 TWCU ThresholdPercentage (組 Config 預設值：80) 參數。實際值應反映貴組織的政策。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | lambda-concurrency-check | 此規則可確保建立 Lambda 函數的並行上限和下限。這可為函數在任何指定時間服務的請求數設定基準。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | rds-enhanced-monitoring-enabled | 啟用 Amazon Relational Database Service (Amazon RDS) 可協助監控 Amazon RDS 的可用性。這可讓您詳細掌握 Amazon RDS 資料庫執行個體的運作狀態。當 Amazon RDS 儲存體使用多個基礎實體裝置時，增強型監控會收集每部裝置的資料。此外，當 Amazon RDS 資料庫執行個體在多可用區部署中執行時，就會收集次要主機上每部裝置的資料，以及次要主機指標。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.1 | IT 系統應隨著 NBFC 營運規模和複雜性增加而逐步擴展。 | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 會從多個服務彙總、組織和排列安全性警示或發現項目的優先順序。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie， AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | dms-replication-not-public | 確保 DMS 複寫執行個體無法公開存取，以管理對 AWS 雲端的存取。DMS 複寫執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | ebs-snapshot-public-restorable-check | 確保 EBS 快照不可公開還原，以管理對 AWS 雲端的存取。EBS 磁碟區快照可能包含敏感資訊，此類帳戶需要存取控制。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | elasticsearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務（服 OpenSearch 務）域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 OpenSearch 服務網域可讓 Amazon VPC 內的 OpenSearch 服務與其他服務之間的安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | emr-master-no-public-ip | 透過確保 Amazon EMR 叢集主節點無法公開存取，以管理對 AWS 雲端的存取。Amazon EMR 叢集主節點可能包含敏感資訊，此類帳戶需要存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | internet-gateway-authorized-vpc-only | 透過確保網際網路閘道僅連接到授權的 Amazon 虛擬私有雲端 (Amazon VPC)，以管理雲端資源的存取。AWS 網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | rds-instance-public-access-check | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | rds-snapshots-public-prohibited | 透過確保 Amazon 關聯式資料庫服務 (Amazon RDS) 執行個體不是公開的，來管理 AWS 雲端中資源的存取。Amazon RDS 資料庫執行個體可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | redshift-cluster-public-access-check | 透過確保 Amazon Redshift 叢集不是公開的，來管理 AWS 雲端中資源的存取。Amazon Redshift 叢集可能包含敏感資訊和原則，此類帳戶需要原則和存取控制。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | s3-account-level-public-access-blocks-periodic | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、 blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | sagemaker-notebook-no-direct-internet-access | 確保 Amazon SageMaker 筆記本電腦不允許直接存取網際網路，以管理 AWS 雲端資源的存取。透過防止直接存取網際網路，您可以避免未經授權的使用者存取敏感資料。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | emr-kerberos-enabled | 透過啟用適用於 Amazon EMR 叢集的 Kerberos，即可利用最低權限和職責分離的原則來管理並整合存取許可和授權。Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在這個領域內，Kerberos 伺服器稱為金鑰分佈中心 (KDC)。其為主體提供驗證的方法。KDC 的驗證做法是發出票證來進行驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | autoscaling-launch-config-public-ip-disabled | 如果您使用公有 IP 地址設定網路介面，則可從網際網路存取這些網路介面的相關聯資源。EC2 資源不可公開存取，因為這可能會導致意外存取應用程式或伺服器。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | ecs-task-definition-nonroot-user | 為了協助實作最低權限原則，請確保已指定非根使用者來存取 Amazon Elastic Container Service (Amazon ECS) 任務定義。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | efs-access-point-enforce-root-directory | 針對 Amazon Elastic File System (Amazon EFS) 存取點強制執行根目錄，可確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | efs-access-point-enforce-user-identity | 為了協助實作最低權限原則，請確保已為 Amazon Elastic File System (Amazon EFS) 啟用使用者強制執行。啟用後，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為所有檔案系統操作之存取點上設定的身分，並且僅授予對此強制使用者身分的存取權。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | s3-bucket-level-public-access-prohibited | 透過確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | subnet-auto-assign-public-ip-disabled | 透過確保 Amazon 虛擬私有 AWS 雲端 (VPC) 子網路不會自動指派公用 IP 位址，以管理對雲端的存取。在啟用此屬性的子網路中啟動的 Amazon Elastic Compute Cloud (EC2) 執行個體，具有指派給其主要網路介面的公有 IP 地址。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權限，可以控制系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶來幫助納入最少功能的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。要求使用者使用 MFA 以減少帳戶遭到入侵的事件。 |
| 8.I | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。MFA 在登入憑證之外多加了一層保護。透過要求使用者使用 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | root-account-hardware-mfa-enabled | 透過確保針對 root 使用者啟用硬體 MFA，來管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | opensearch-in-vpc-only | 通過確保 Amazon OpenSearch 服務域位於 Amazon Virtual Private Cloud（Amazon VPC）中來管理對雲的訪問。 AWS Amazon VPC 中的 Amazon OpenSearch 服務網域可讓 Amazon OpenSearch 服務與 Amazon VPC 內的其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | root-account-mfa-enabled | 確保針對 root 使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 8.l | 基本安全方面，例如實體/邏輯存取控制和明確定義的密碼政策。 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.II | 明確定義的使用者角色。 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 8.II | 明確定義的使用者角色。 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.II | 明確定義的使用者角色。 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.II | 明確定義的使用者角色。 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) 可協助您將最低權限和職責分離的原則與存取權限和授權結合，限制政策不包含「效果」：「允許」與「動作」：「*」而非「資源」：「*」。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 8.II | 明確定義的使用者角色。 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.II | 明確定義的使用者角色。 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 8.II | 明確定義的使用者角色。 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage 年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.III | 可降低錯誤和濫用的風險，並確保資料/資訊可靠性的經辦者/審核者 (Maker-checker) 概念。 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 8.IX | 安排進行資料備份並定期測試。 | db-instance-backup-enabled | Amazon RDS 的備份功能可建立資料庫和交易日誌的備份。Amazon RDS 會自動建立資料庫執行個體的儲存磁碟區快照，並備份整個資料庫執行個體。系統可讓您設定特定的保留期間，以符合您的恢復能力要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.IX | 安排進行資料備份並定期測試。 | dynamodb-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon DynamoDB 表是備份計劃的一 AWS 部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.IX | 安排進行資料備份並定期測試。 | dynamodb-pitr-enabled | 啟用此規則可檢查資訊是否已備份。它也會透過確保在 Amazon DynamoDB 中啟用 point-in-time 復原功能來維護備份。復原會維護資料表在過去 35 天內的連續備份。 |
| 8.IX | 安排進行資料備份並定期測試。 | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.IX | 安排進行資料備份並定期測試。 | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.IX | 安排進行資料備份並定期測試。 | elasticache-redis-cluster-automatic-backup-check | 啟用自動備份後，Amazon ElastiCache 會每天建立叢集的備份。備份保留天數由貴組織指定。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新叢集，從最新的備份還原您的資料。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.IX | 安排進行資料備份並定期測試。 | rds-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Relational Database Service (Amazon RDS) 執行個體是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 8.IX | 安排進行資料備份並定期測試。 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (CRR) 可讓您維持足夠的容量和可用性。CRR 支援跨 Amazon S3 儲存貯體自動非同步複製物件，以協助確保維持資料可用性。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.IX | 安排進行資料備份並定期測試。 | redshift-backup-enabled | 請確保 Amazon Redshift 叢集具有自動快照，以利處理資料備份。當叢集的自動快照已啟用時，Redshift 將定期為該叢集拍攝快照。根據預設，Redshift 會針對每個資料變更節點 (或以先到者為準) 每 8 小時或每 5 GB 擷取一次快照。 |
| 8.IX | 安排進行資料備份並定期測試。 | backup-plan-min-frequency-and-min-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份計劃設定為最低頻率和保留頻率。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則允許您設置 requiredFrequencyValue（Config 默認值：1），requiredRetentionDays（Config 默認值：35）和 requiredFrequencyUnit（Config 默認值：天）參數。實際值應反映貴組織的要求。 |

| 控制 ID | 控制描述 | AWS Config 規則 | 指引 |
| --- | --- | --- | --- |
| 8.IX | 安排進行資料備份並定期測試。 | backup-recovery-point-manual-deletion-disabled | 確保您的 AWS Backup 復原點具有附加的資源型政策，以防止刪除復原點。使用資源型政策防止刪除復原點，有助於防止意外或故意刪除。 |
| 8.IX | 安排進行資料備份並定期測試。 | backup-recovery-point-minimum-retention-check | 若要協助進行資料 Backup 程序，請確定您的 AWS 備份復原點設定了最短的保留期。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。此規則可讓您設定 requiredRetentionDays (組態預設值：35) 參數。實際值應反映貴組織的要求。 |

### 範本

該模板可在以下位置獲得 GitHub：RBI MD-ITF 的操作最佳實踐。

## 安全、身分及合規服務的最佳實務

此一致性套件包含以「安全性」、「身分識別」和「合 AWS Config 規性服務」為基礎的規則 如需詳細資訊，請參閱上的安全性、身分識別和符合性 AWS。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在下列網站取得 GitHub：安全性、身分識別和合規性服務的最佳作法。

## 無伺服器的操作最佳實務

此一致性套件包含以無伺服器解決方案為基礎的 AWS Config 規則。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本位於 GitHub：無伺服器的營運最佳作法。

## 儲存服務的操作最佳實務

此一致性套件包含以儲存服務為基礎的 AWS Config 規則。如需詳細資訊，請參閱上的雲端儲存 AWS。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本位於 GitHub：儲存服務的營運最佳作法。

## SWIFT CSP 的操作最佳實務

一致性套件提供一般用途的合規性架構，可讓您使用受管或自 AWS Config 訂規則和補救動作來建立安全性、作業或成本最佳化治理檢查。 AWS Config 一致性套件 (作為範例範本) 並不是為了完全確保符合特定控管或合規標準而設計。您有責任自行評估服務的使用情形是否符合適用的法律和法規要求。

下列提供了 SWIFT 客戶安全計劃 (CSP) 和 AWS 受管 Config 規則之間的範例映射。每個 AWS Config 規則都會套用至特定 AWS 資源，並與一或多個 SWIFT CSP 控制項相關。SWIFT CSP 控制項可以與多個 AWS Config 規則相關聯。如需與這些映射相關的詳細資訊和指引，請參閱下方資料表。

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.1 | ec2-instance-managed-by-systems-manager | 透過使用 AWS Systems Manager 管理 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，即可清查組織內的軟體平台和應用程式。使用 AWS Systems Manager 來 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| | | 提供詳細的系統組態、作業系統修補程式等級、服務名稱和類型、軟體安裝、應用程式名稱、發行者和版本，以及環境的其他詳細資料。 |
| 1.1 | ec2-instance-no-public-ip | 確保亞馬遜彈性運算 AWS 雲端 (Amazon EC2) 執行個體無法公開存取，以管理對雲端的存取。Amazon EC2 執行個體可能包含敏感資訊，此類帳戶需要存取控制。 |
| 1.1 | ec2-no-amazon-key-pair | 此規則會檢查是否使用 Amazon 金鑰對啟動 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。這有助於降低憑證遭到入侵的風險。不含金鑰配對的 Amazon EC2 執行個體仍可透過主控台使用工作階段管理員或以瀏覽器為基礎的 AWS SSH 連線存取。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.1 | ec2-instances-in-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 內部署 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，以在 Amazon VPC 內的執行個體與其他服務之間進行安全通訊，不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。將 Amazon EC2 執行個體指派給 Amazon VPC 以正確管理存取權。 |
| 1.1 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可以透過對資源的輸入和輸出網路流量進行有狀態篩選，協助管理網路存取。 AWS 限制預設安全群組上的所有流量有助於限制對資源的遠端存 AWS 取。 |
| 1.1 | vpc-network-acl-unused-check | 此規則可確保正在使用 Amazon Virtual Private Cloud (VPC) 網路存取控制清單。監控未使用的網路存取控制清單，可協助您的環境進行準確的清查和管理。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.1 | vpc-sg-open-only-to-authorized-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。透過限制從網際網路 (0.0.0.0/0) 存取安全群組內的資源，可以控制內部系統的遠端存取。 |
| 1.2 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) 可協助您將最低權限和責任分離的原則與存取權限和授權結合在一起，從而限制政策對所有 AWS 金鑰管理服務金鑰包含封鎖的動作。擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.2 | iam-group-has-users-check | AWS Identity and Access Management (IAM) 可確保 IAM 群組至少有一位使用者，協助您將最低權限和職責分離的原則與存取權限和授權結合在一起。根據使用者的相關許可或工作職能將使用者放入群組中是整合最低權限的一種方法。 |
| 1.2 | iam-inline-policy-blocked-kms-actions | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策，允許對所有 AWS 金鑰管理服務金鑰執行封鎖動作。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。此規則可讓您設定 blockedActionsPatterns 參數。(AWS 基礎安全性最佳做法值：KMS: 解密，公里：寄件者)。ReEncrypt實際值應反映貴組織的政策。 |
| 1.2 | iam-no-inline-policy-check | 確保 I AWS dentity and Access Management (IAM) 使用者、IAM 角色或 IAM 群組沒有內嵌政策來控制系統和資產的存取。 AWS 建議使用受管理的政策，而非內嵌政策。受管政策允許執行重複使用、版本控制、復原及委派許可管理功能。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.2 | iam-user-no-policies-check | 此規則可確保 AWS Identity and Access Management (IAM) 政策僅附加至群組或角色，以控制對系統和資產的存取。在群組或角色層級指派權限，有助於降低某身分收到或保留過多權限的機會。 |
| 1.2 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) 安全群組可針對資源的輸入和輸出網路流量提供狀態篩選，協助管理網路存取。 AWS 不允許資源從 0.0.0.0/0 到連接埠 22 的輸入 (或遠端) 流量，有助於限制遠端存取。 |
| 1.2 | nacl-no-unrestricted-ssh-rdp | 網路存取控制清單 (NACL) 中的遠端伺服器管理連接埠 (例如連接埠 22 (SSH) 和連接埠 3389 (RDP)) 不應可公開存取，因為這可能會允許 VPC 內資源的非預期存取。 |
| 1.2 | s3-bucket-acl-prohibited | 此規則會檢查存取控制清單 (ACL) 是否用於在 Amazon S3 儲存貯體上進行存取控制。ACL 是 Amazon S3 儲存貯體的舊版存取控制機制，早於 AWS Identity and Access Management (IAM)。最佳實務是使用 IAM 政策或 S3 儲存貯體政策，更輕鬆地管理 S3 儲存貯體的存取，而非使用 ACL。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.2 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) 伺服器存取日誌記錄提供了可監控網路是否存在潛在網路安全事件的方法。透過擷取發出至 Amazon S3 儲存貯體的請求詳細記錄以監控事件。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊。詳細資訊包括請求者、儲存貯體名稱、請求時間、請求動作、回應狀態，以及相關的錯誤代碼。 |
| 1.2 | s3-bucket-policy-grantee-check | 通過啟用 s3_ 保險政策檢查來管理對 AWS 雲的訪問。此規則會檢查 Amazon S3 儲存貯體授與的存取權是否受到您提供的任何 AWS 主體、聯合身分使用者、服務主體、IP 地址或 Amazon Virtual Private Cloud (Amazon VPC) ID 的限制。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.2 | sns-topic-message-delivery-notification-enabled | 為了協助達成環境中的日誌記錄要求，請確保針對 Amazon Simple Notification Service (Amazon SNS) 主題啟用傳遞狀態通知。日誌記錄訊息傳遞狀態有助於提供更好的操作洞察功能，例如：了解訊息是否已傳遞至 Amazon SNS 端點、識別從 Amazon SNS 端點傳送至 Amazon SNS 的回應，以及判斷訊息暫留時間 (從發佈時間戳記到移交給 Amazon SNS 端點之前的時間)。 |
| 1.4 | internet-gateway-authorized-vpc-only | 確保網際網路閘道僅連接至授權的 Amazon 虛擬私有 AWS 雲端 (Amazon VPC)，以管理雲端資源的存取。網際網路閘道允許進出 Amazon VPC 的雙向網際網路存取，這可能導致未經授權存取 Amazon VPC 資源。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.4 | restricted-common-ports | 透過確保 Amazon 彈性運算 AWS 雲端 (Amazon EC2) 安全群組上的通用連接埠受到限制，以管理雲端中資源的存取。如果不將連接埠的存取限制為信任來源，可能會導致系統的可用性、完整性和機密性遭到攻擊。此規則可讓您選用設定 blockedPort1 - blockedPort5 參數 (Config 預設值：20、21、3389、3306、4333)。實際值應反映貴組織的政策。 |
| 1.4 | lambda-function-public-access-prohibited | 確保 AWS Lambda 函數無法公開存取，以管理對 AWS 雲端資源的存取。公開存取可能會導致資源可用性降低。 |
| 1.4 | s3-account-level-public-access-blocks-periodic | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止公開存取，避免未經授權的遠端使用者存取敏感資料。此規則可讓您選擇性地設定 ignorePublicAcls (組 Config 預設值：True)、blockPublicPolicy (組 Config 預設值：True)、 blockPublicAcls (組 Config 預設值：True) 和 restrictPublicBuckets 參數 (組 Config 預設值：True)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 1.4 | s3-bucket-level-public-access-prohibited | 確保 Amazon Simple Storage Service (Amazon S3) 儲存貯體無法公開存取，以管理 AWS 雲端中資源的存取。此規則可透過防止儲存貯體層級的公開存取，避免未經授權的遠端使用者存取敏感資料。 |
| 1.4 | s3-bucket-public-read-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.4 | s3-bucket-public-write-prohibited | 只允許授權的使用者、程序和裝置存取 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以管理 AWS 雲端中資源的存取。存取管理應與資料的分類一致。 |
| 1.4 | ssm-document-not-public | 請確定 AWS Systems Manager (SSM) 文件不是公開的，因為這可能會允許意外存取您的 SSM 文件。公有 SSM 文件可能會公開帳戶、資源和內部程序的相關資訊。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.3 | ec2-imdsv2-check | 確保啟用執行個體中繼資料服務第 2 版 (IMDSv2) 方法可協助保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體中繼資料的存取和控制。IMDSv2 方法使用工作階段型控制項。透過 IMDSv2，您可以實作這些控制以限制執行個體中繼資料的變更。 |
| 2.3 | ec2-instance-multiple-eni-check | 此規則會檢查您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體是否擁有多個 ENI。擁有多個 ENI 可能會導致雙主目錄執行個體，也就是具有多個子網路的執行個體。這可能會增加網路安全複雜性，並導致意外的網路路徑和存取。 |
| 2.3 | ec2-token-hop-limit-check | 確保執行個體中繼資料服務 (IMDS) HTTP PUT 回應僅限於 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。使用 IMDSv2 時，因為中繼資料回應躍點限制設定為 1 (Config 預設值)，所以預設會包含密碼字符的 PUT 回應無法傳送到執行個體之外。如果此值大於 1，則字符可以傳送出 EC2 執行個體。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.3 | ec2-volume-inuse-check | 此規則可確保在執行個體終止時，連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store 磁碟區會被標記為待刪除。如果 Amazon EBS 磁碟區在其連接的執行個體終止時未予以刪除，則可能會違反最少功能的概念。 |
| 2.3 | account-part-of-organizations | 在 Organ AWS izations AWS 帳戶 內部集中管理有助於確保帳戶符合規定。缺乏集中式帳戶控管可能會導致帳戶組態不一致，這可能會公開資源和敏感資料。 |
| 2.3 | lambda-inside-vpc | 在 Amazon Virtual Private Cloud (Amazon VPC) 中部署 AWS Lambda 函數，以便在 Amazon VPC 內的函數與其他服務之間進行安全通訊。有了這項組態，就不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。相較於使用公有端點的網域，位於 Amazon VPC 內的網域因為提供邏輯隔離，所以多了一層安全防護。若要正確管理存取，應將 AWS Lambda 函數指派給 VPC。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.3 | kms-cmk-not-scheduled-for-deletion | 若要協助保護靜態資料，請確定金鑰管理服務 (AWS KMS) 中未排程刪除必要的客戶主金 AWS 鑰 (CMK)。因為刪除金鑰有時為必要，而這個規則可協助檢查所有排程要刪除的金鑰，以防無意中排程刪除金鑰。 |
| 2.3 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) 儲存貯體版本控制可協助您將物件的多個變體儲存在同一個 Amazon S3 儲存貯體中。請使用版本控制功能來保留、擷取和還原存放在 Amazon S3 儲存貯體中之每個物件的每個版本。版本控制可協助您輕鬆從意外的使用者動作和應用程式失敗中復原。 |
| 2.3 | secretsmanager-secret-unused | 如果 AWS Secrets Manager 中存在未使用的認證，您應該停用和/或移除認證，因為這可能會違反最低權限原則。此規則可讓您將值設定為 unusedForDays (組 Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5A | ebs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |
| 2.5A | ec2-ebs-encryption-by-default | 為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。由於這些磁碟區中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.5A | efs-encrypted-check | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic File System (EFS) 啟用加密功能。 |
| 2.5A | efs-in-backup-plan | 為了協助進行資料 Backup 程序，請確保您的 Amazon Elastic File System (Amazon EFS) 檔案系統是 AWS 備份計劃的一部分。 AWS Backup 是一種全受管備份服務，具有原則型備份解決方案。此解決方案可簡化備份管理，讓您達到業務與法規的備份合規要求。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 2.5A | encrypted-volumes | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密功能。 |
| 2.5A | kinesis-stream-encrypted | 由於可能存在敏感資料，因此為了協助保護靜態資料，請確保已針對 Amazon Kinesis Streams 啟用加密功能。 |
| 2.5A | s3-bucket-server-side-encryption-enabled | 為了協助保護靜態資料，請確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用加密以協助保護該資料。 |
| 2.5A | s3-default-encryption-kms | 確保已針對 Amazon Simple Storage Service (Amazon S3) 儲存貯體啟用加密功能。由於 Amazon S3 儲存貯體中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 2.5A | sns-encrypted-kms | 為了保護靜態資料，請確保您的 Amazon Simple Notification Service (Amazon SNS) 主題需要使用金 AWS 鑰管理服務 (AWS KMS) 進行加密。由於已發布訊息中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.1 | iam-password-policy | 身分和憑證會依組織的 IAM 密碼政策核發、管理及驗證。它們符合或超過 NIST SP 800-63 和密碼強度 AWS 基礎安全性最佳實務標準所述的要求。此規則可讓您選擇性地設定 RequireUppercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireLowercaseCharacters (AWS 基礎安全最佳做法值：true)、 RequireSymbols (AWS 基礎安全最佳做法值：true)、 RequireNumbers (AWS 基礎安全最佳做法值：true)、 MinimumPasswordLength (AWS 基礎安全最佳實務值：14)、(基礎安全性最佳實務值：24) 和 PasswordReusePrevention MaxPasswordAge (AWS IAM 的最佳實務值：90)AWS 密碼策略。實際值應反映貴組織的政策。 |
| 4.1 | access-keys-rotated | 透過確保按照組織政策的指定輪替 IAM 存取金鑰，以針對授權的裝置、使用者和程序稽核登入資料。定期變更存取金鑰是安全最佳實務。這可縮短存取金鑰的作用中時間，並在金鑰洩漏時降低業務影響。此規則需要存取金鑰輪換值 (Config 預設值：90)。實際值應反映貴組織的政策。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.2 | iam-user-mfa-enabled | 啟用此規則可限制對 AWS 雲端中資源的存取。此規則可確保為所有使用者都啟用了多重要素驗證 (MFA)。MFA 在登入憑證之上增加了一層額外的保護。透過為使用者要求 MFA 來減少帳戶遭到入侵的事件。 |
| 4.2 | mfa-enabled-for-iam-console-access | 透過確保對具有主控台密碼的所有 AWS Identity and Access Management (IAM) 使用者啟用 MFA，以管理 AWS 雲端資源的存取。MFA 在登入憑證之外多加了一層保護。透過為使用者要求 MFA，您可以減少帳戶遭到入侵的事件，並防止未經授權的使用者存取敏感資料。 |
| 4.2 | root-account-hardware-mfa-enabled | 確保針對 root 使用者啟用硬體 MFA，以管理 AWS 雲端資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 4.2 | root-account-mfa-enabled | 確保針對根使用者啟用 MFA，以管理 AWS 雲端中資源的存取。根使用者是 AWS 帳戶中權限最高的使用者。MFA 為登入憑證多增加一層保護。透過針對 root 使用者要求 MFA，您可以減少遭到入侵 AWS 帳戶的事件。 |
| 5.1 | ec2-instance-profile-attached | EC2 執行個體設定檔可將 IAM 角色傳遞給 EC2 執行個體。將執行個體設定檔連接到執行個體可協助管理最低權限和許可。 |
| 5.1 | iam-policy-no-statements-with-full-access | 確保 IAM 動作僅限於需要的動作。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 5.1 | iam-root-access-key-check | 透過檢查 root 使用者是否沒有附加到其 AWS 身分識別和存取管理 (IAM) 角色的存取權，可以控制對系統和資產的存取。請確保已刪除根存取金鑰。相反，創建和使用基於角色 AWS 帳戶 來幫助納入最少功能的原則。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 5.1 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) 可協助您限制存取權限和授權，方法是確保使用者至少是一個群組的成員。允許使用者擁有超過完成任務所需的權限，可能會違反最低權限和職責分離的原則。 |
| 5.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) 可以透過檢查指定時段未使用的 IAM 密碼和存取金鑰來協助您取得存取許可和授權。如果識別出這些未使用的憑證，建議您停用和/或移除憑證，因為這可能會違反最低權限的原則。此規則要求您將值設置為 maxCredentialUsage年齡（Config 默認值：90）。實際值應反映貴組織的政策。 |
| 5.4 | secretsmanager-rotation-enabled-check | 此規則可確保 AWS Secrets Manager 密碼已啟用循環。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。 |
| 5.4 | secretsmanager-scheduled-rotation-success-check | 此規則可確保 AWS Secrets Manager 密碼已根據循環排程成功輪替。定期輪換密碼可縮短密碼處於作用中的時間，並可能降低密碼洩露時所造成的業務影響。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 5.4 | secretsmanager-secret-periodic-rotation | 此規則可確保「AWS Secrets Manager」密碼已啟用定期輪換。定期輪換密碼可縮短密碼的作用中時間，並可能降低密碼洩漏時所造成的業務影響。預設值為 90 天。 |
| 5.4 | secretsmanager-using-cmk | 若要協助保護靜態資料，請確定 AWS Secrets Manager 密碼已啟用金 AWS 鑰管理服務 (AWS KMS) 的加密功能。由於 Secrets Manager 密碼中可能存在靜態敏感資料，因此請啟用靜態加密以協助保護該資料。 |
| 6.4 | ec2-instance-detailed-monitoring-enabled | 啟用此規則可協助改善 Amazon EC2 主控台上的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體監控，並顯示執行個體以 1 分鐘為區間的監控圖形。 |
| 6.4 | cloudwatch-log-group-encrypted | 為了協助保護靜態敏感資料，請確保已為 Amazon CloudWatch 日誌群組啟用加密。 |
| 6.4 | cloud-trail-cloud-watch-logs-enabled | 使用 Amazon CloudWatch 集中收集和管理日誌事件活動。包含 AWS CloudTrail 資料可提供您的 AWS 帳戶. |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4 | cloudtrail-enabled | AWS CloudTrail 可以透過記錄 AWS 管理主控台動作和 API 呼叫來協助不可否認性。您可以識別使用者 AWS 帳戶 以及呼叫 AWS 服務的使用者、產生呼叫的來源 IP 位址，以及呼叫的計時。捕獲的數據的詳細信息可以在 AWS CloudTrail 記錄內容中看到。 |
| 6.4 | cloud-trail-encryption-enabled | 由於敏感資料可能存在並協助保護靜態資料，因此請確保 AWS CloudTrail 追蹤已啟用加密功能。 |
| 6.4 | cloud-trail-log-file-validation-enabled | 利用日 AWS CloudTrail 誌文件驗證來檢查 CloudTrail 日誌的完整性。記錄檔驗證有助於判斷記錄檔在 CloudTrail 傳送之後是否已修改或刪除或未變更。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。 |
| 6.4 | ec2-stopped-instance | 啟用此規則可根據組織的標準，檢查 Amazon EC2 執行個體的停止時間是否超過允許的天數，藉以設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的基準組態。 |

| 控制 ID | AWS Config 規則 | 指引 |
| --- | --- | --- |
| 6.4 | vpc-flow-logs-enabled | VPC 流程日誌可以提供 Amazon Virtual Private Cloud (Amazon VPC) 中網路介面 IP 流量傳入及傳出的相關資訊詳細記錄。根據預設，流程日誌記錄包含 IP 流程不同元件的值，包括來源、目標和通訊協定。 |
| 6.5A | guardduty-enabled-centralized | Amazon GuardDuty 可以使用威脅情報摘要，協助監控和偵測潛在的網路安全事件。其中包括惡意 IP 和機器學習列表，用於識別 AWS 雲端環境中的未預期、未經授權和惡意活動。 |
| 6.5A | securityhub-enabled | AWS Security Hub 有助於監控未經授權的人員，連接，設備和軟件。 AWS Security Hub 彙總、組織和優先處理來自多個服務的安全性警示或發現項目。 AWS 一些這樣的服務是 Amazon Security Hub，Amazon Inspector，Amazon Macie，AWS Identity and Access Management (IAM) 訪問分析器， AWS Firewall Manager 器和 AWS 合作夥伴解決方案。 |

## 範本

該模板可用於 GitHub：SWIFT CSP 的操作最佳實踐。

## Amazon Elastic Container Service (Amazon ECS) 的安全最佳實務

此一致性套件包含以 Amazon ECS 為基礎的 AWS Config 規則。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：適用於 Amazon ECS 的安全最佳實務。

## Amazon Elastic File System (Amazon EFS) 的安全最佳實務

此一致性套件包含以 Amazon EFS 為基礎的 AWS Config 規則。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

範本可在以下網站取得 GitHub：適用於 Amazon EFS 的安全性最佳實務。

## Amazon Elastic Kubernetes Service (Amazon EKS) 的安全最佳實務

此一致性套件包含以 Amazon EKS 為基礎的 AWS Config 規則。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可在以下位置找到 GitHub：Amazon EKS 的安全最佳實踐。

## Amazon 的安全最佳實踐 CloudFront

此一致性包包含基於 Amazon 的 AWS Config 規則。 CloudFront如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可用於 GitHub：Amazon 的安全最佳實踐 CloudFront。

## Amazon OpenSearch 服務的安全最佳實踐

此一致性包包含基於 Amazon OpenSearch 服務的 AWS Config 規則。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可用於 GitHub：Amazon OpenSearch 服務的安全最佳實踐。

## Amazon Redshift 的安全最佳實務

此一致性包包含基於 Amazon Redshift 的 AWS Config 規則。如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可在以下位置找到 GitHub：Amazon Redshift 的安全最佳實踐。

## Amazon Relational Database Service (Amazon RDS) 的安全最佳實務

此一致性套件包含以 Amazon RDS 為基礎的 AWS Config 規則。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：適用於 Amazon RDS 的安全最佳實務。

## AWS Auto Scaling的安全最佳實務

此符合性套件包含 AWS Config 以. AWS Auto Scaling如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：的安全最佳做法 AWS Auto Scaling。

## AWS CloudTrail的安全最佳實務

此符合性套件包含 AWS Config 以. AWS CloudTrail如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：的安全最佳做法 AWS CloudTrail。

## AWS CodeBuild的安全最佳實務

此符合性套件包含 AWS Config 以. AWS CodeBuild如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：的安全最佳做法 AWS CodeBuild。

## Amazon ECR 的安全最佳實務

此一致性包包含基於 Amazon Elastic Container Registry (Amazon ECR) 的 AWS Config 規則。如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：適用於 Amazon ECR 的安全最佳實務。

## AWS Lambda的安全最佳實務

此符合性套件包含 AWS Config 以. AWS Lambda如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：的安全最佳做法 AWS Lambda。

## AWS Network Firewall的安全最佳實務

此符合性套件包含 AWS Config 以. AWS Network Firewall如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：的安全最佳做法 AWS Network Firewall。

## Amazon 的安全最佳實踐 SageMaker

此一致性包包含基於 Amazon 的 AWS Config 規則。 SageMaker如需支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該模板可用於 GitHub：Amazon 的安全最佳實踐 SageMaker。

## AWS Secrets Manager的安全最佳實務

此符合性套件包含 AWS Config 以. AWS Secrets Manager如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：的安全最佳做法 AWS Secrets Manager。

## AWS WAF的安全最佳實務

此符合性套件包含 AWS Config 以. AWS WAF如需受支援的所有受管規則清單 AWS Config，請參閱AWS Config 受管規則清單。

如需必要參數的名稱和描述，請參閱下列範本中的一`Parameters`節。

該範本可在以下網站取得 GitHub：的安全最佳做法 AWS WAF。

## 具有修補動作的範例範本

### 具有修復功能的 Amazon DynamoDB 最佳作法

該模板可用於 GitHub：具有修復功能的 Amazon DynamoDB 最佳作法。

### 具有修復功能的 Amazon S3 營運最佳實務

該模板可用於 GitHub：具有修復功能的 Amazon S3 營運最佳實務。

如需範本結構的詳細資訊，請參閱《AWS CloudFormation使用指南》中的〈範本剖析〉。

# 自訂一致性套件

自訂一致性套件是 AWS Config 規則和修正動作的唯一集合，您可以在帳戶和 AWS 區域中一起部署，或在中的組織中部署。 AWS Organizations

若要製作自訂一致性套件，請遵循下列自訂範本一節中的步驟，撰寫您要使用的 YAML 檔案，其包含AWS Config 受管規則 或 AWS Config 自訂規則清單。

## 術語

AWS Config 受管規則是擁有的預先定義規則 AWS Config。

AWS Config 自訂規則是您從頭開始建立的規則。

建立 AWS Config 自訂規則的方法有兩種：使用 Lambda 函數 (AWS Lambda 開發人員指南)，以及使用 Guard (安全防護 GitHub儲存庫) (一種 policy-as-code 語言)。 AWS Config 使用建立的自訂規 AWS Lambda 則稱為AWS Config 自訂 Lambda 規則，而 AWS Config 使用安全警衛建立的自訂規則稱為AWS Config 自訂原則規則。

## 自訂範本

建立您的 YAML 檔案

若要建立 YAML 檔案，請開啟文字編輯器，並將檔案儲存為 .yaml。

> **Note**
>
> 您的檔案將包含參數和資源區段。

參數

YAML 檔案中的`Parameters`區段適用於您稍後將在`Resources`區段中新增之 AWS Config 規則集的規則參數。藉由將下列程式碼區塊複製並貼至 YAML 檔案中，並視需要進行自訂，且針對每個規則參數重複此步驟，即可建立 `Parameters` 區段。

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

例如：

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> 選取要建立自訂一致性套件的 AWS Config 規則時，請檢查您的帳戶中是否已佈建要針對規則進行評估的 AWS Config 資源。

1. 之後的參數部分的第一行`Parameters:`是 + 參數 *`NameOfRule`*+ 的連接字符串。*`NameOfRuleParameter`*
   a. 以您為規則建立的一致名稱取代 *`NameOfRule`*。例如，這可能是IamPasswordPolicy為了iam-password-policy 規則。
   b. 輸入 `Param`。
   c. 然後，以指定規則的規則參數名稱取代 *`NameOfRuleParameter`*。對於 AWS Config 受管規則，規則參數的名稱位於AWS Config 受管規則清單中 (例如，MinimumPasswordLength是規則的規則參數名稱)。iam-password-policy若為 AWS Config 自訂規則，則規則參數名稱是您在建立規則時選擇的名稱。
2. 如果您使用的是受 AWS Config 管規則，請在受管規 AWS Config 則清單中尋找適當的規則，以便瞭解特定規則`Default`和特定規則`Type`的接受值。若為 AWS Config 自訂規則，請使用您在建立規則時選取的值。

   > **Note**
   >
   > `Type`必須為每個參數指定。 `Type`可以是「字符串」，「整數」，「雙」，「CSV」，「布爾」和「」StringMap 之一。

資源

此 `Resources` 區段會列出新增至「自訂一致性套件」的規則。直接在 `Parameters` 區段下方新增下列 `Resources` 區塊，並視需要進行自訂，且針對每個規則重複此步驟。如需規格的詳細資訊，請參閱AWS::Config::ConfigRule。

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: NameOfRuleParamNameOfRuleParameter
```

```
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
    ...
```

例如：

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> 選取要建立自訂一致性套件的 AWS Config 規則時，請檢查您是否具有針對帳戶中佈建的 AWS Config 規則進行評估的資源。如需詳細資訊，請參閱支援的資源類型。

1. 以您在 `Parameters` 區段中建立的相同名稱取代 *`NameOfRule`*。
2. 對於 AWS Config 受管規則，請*`ActualConfigRuleName`*以受AWS Config 管規則清單上適當規則頁面的標題取代。對於 AWS Config 自訂規則，請使用您在規則建立時選擇的 Config 規則名稱。
3. 以您在 `Parameters` 區段中使用的相同名稱取代 *`NameOfRuleParameter`*。冒號後，複製並粘貼您在部分中創建的 *`NameOfRule`*+ 參數 + 相同的連接字符串。*`NameOfRuleParameter`*`Parameters`
4. 將 *`Owner`* 變更為適當的值。

> **Note**
>
> AWS Config 受管規則
> 對於 AWS Config 受管規則，`Owner`的值為`AWS`。

AWS Config 自訂規則
對於使用安全警衛建立的 AWS Config 自訂規則，的值為`OwnerCUSTOM_POLICY`。對於使用 Lambda 建立的 AWS Config 自訂規則，的值為`OwnerCUSTOM_LAMBDA`。

5. 將 *`SOURCE_IDENTIFIER`* 變更為適當的值。

> **Note**
>
> AWS Config 受管規則
> 針對 AWS Config 受管規則，請遵循您從「受AWS Config 管規則清單」中選取之規則的連結 (例如，規則的來源識別碼為 ACCESS_KEYS_SELE CTION)，複製識別碼。access-keys-rotated
> AWS Config 自訂規則
> 對於使用 Lambda 建立的 AWS Config 自訂規則，則`SourceIdentifier`是規則 AWS Lambda 函數的 Amazon 資源名稱 (ARN)，例如`arn:aws:lambda:us-east-2:123456789012:function:`*`ActualConfigRuleName`*. 對於使用安全警衛建立的 AWS Config 自訂規則，不需要此欄位。

總之，您填寫的自訂一致性套件應該會開始看起來類似下列內容，這是使用這些 AWS Config 受管規則的範例：iam-password-policyaccess-keys-rotated、和 iam-user-unused-credentials-check。

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
```

```
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge:
IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

## 部署您的自訂一致性套件

若要部署您的自訂一致性套件，請參閱使用部署一致性套件 AWS Config 控制台和使用 AWS Config 命令行界面部署一致性包。

# 在一致性套件儀表板中檢視合規資料

一致性套件 的主頁面會顯示 AWS 帳戶 內目前擁有的所有一致性套件。此頁面也包含每個一致性套件的名稱、部署狀態和合規分數。合規分數是一致性套件中合規規則與合規資源組合數目，相較於一致性套件中可能規則與可能資源組合總數的百分比。

您可以使用此儀表板來了解一致性套件的合規性層級，並使用合規分數來追蹤修復進度、執行不同要求集的比較，以及查看特定變更或部署對一致性套件的影響。

## 導覽一致性套件主頁

1. 請登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/config/ 的 AWS Config 主控台。
2. 導覽至 一致性套件 頁面。檢閱您的一致性套件及其合規分數。您也可以須執行下列動作：

- 若要新增和設定新的一致性套件，請選擇 部署一致性套件。
- 若要刪除一致性套件及其資料、變更組態設定或檢視其他詳細資訊 (例如傳送位置或參數)，請選擇一致性套件並選擇 動作。

> **Note**
>
> 您無法編輯已部署的一致性套件。您可以隨時修改其他選取項目，方法是在 動作 下拉式清單中選擇一致性套件的名稱，然後選擇 編輯。

- 若要檢視合規狀態變更的歷史記錄，請選擇一致性套件，然後選擇 一致性套件時間軸。如需詳細資訊，請參閱《檢視一致性套件的合規歷史記錄時間軸》。
- 若要以詳細資訊檢視一致性套件的部署狀態、合規分數、合規分數時間軸及規則，請選擇一個一致性套件，然後選擇 檢視。

## 進一步了解

一致性套件先決條件

一致性套件範例範本

部署一致性套件

AWS 服務限制

# 檢視一致性套件的合規歷史記錄時間軸

AWS Config 支援將合規性狀態變更儲存至您的一致性套件。這可讓您檢視合規狀態變更的歷史記錄。這些合規狀態變更會顯示為時間軸。時間軸會將一段時間內的變更擷取為 `ConfigurationItems`。您也可以使用此功能來尋找符合套件中不相容的特定規則。

您可以選擇使用或選擇退出在 AWS Config中記錄所有資源類型。如果您已選擇記錄所有資源類型，則會根據規則評估， AWS Config 自動開始記錄符合性套件相容性歷史記錄。 AWS Config 依預設，會 AWS Config 記錄所有支援資源的組態變更。您也可以僅選取特定的一致性套件合規歷史記錄資源類型：`AWS::Config::ConformancePackCompliance`。`AWS::Config::ConformancePackCompliance` 資源型態的記錄不會收取額外的費用。如需詳細資訊，請參閱選取哪些資源 AWS Config 記錄。

如果一致性套件中的所有規則都合規，則表示一致性套件為合規。如果有任何規則不合規，則表示一致性套件為不合規。只有當因為資料不足而無法評估一致性套件內的所有規則時，一致性套件的合規狀

態才會是「INSUFFICIENT_DATA」。如果一致性套件中的部分規則合規，但相同一致性套件中其他規則的合規狀態為「INSUFFICIENT_DATA」，則一致性套件會顯示合規。不會一次全部評估一致性套件的合規性。部分規則可能需要比其他規則更長的時間來評估。系統會一次評估一個規則群組的合規性，並分階段繼續進行，直到一致性套件中的所有規則皆經過評估為止。

主題


- 檢視合規時間軸
- 查詢合規歷史記錄


## 檢視合規時間軸

從一致性套件主頁面中選取特定的一致性套件，以存取合規時間軸。

1. 導覽至一致性套件頁面。
2. 在一致性套件主頁上，選擇特定的一致性套件，然後選擇 一致性套件時間軸。

> **Note**
>
> 或者，您也可以從一致性套件的詳細資料頁面內使用合規時間軸。選擇一致性套件，然後在動作 下拉式清單中選擇 檢視詳細資訊。在此頁面中，選擇一致性套件時間軸。

時間軸會顯示一致性套件的合規狀態變更歷史記錄。您可以執行下列作業：

1. 展開規範遵循變更，以檢視符 line-by-line 合性套件中每個規則的符合性狀態。
2. 從展開的檢視中，選擇特定規則以檢視其詳細資訊頁面。

## 查詢合規歷史記錄

使 get-resource-config-history 用資源類型查詢符合性歷史記錄`AWS::Config::ConformancePackCompliance`。

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

您應該會看到類似下列的輸出：

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
```

```
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

如需詳細資訊，請參閱支援的資源類型 (AWS Config) 和 API 參考資料GetResourceConfigHistory中的。

# 使用 AWS Config 主控台部署一致性套件

在 Conformance packs (一致性套件) 頁面上，您可以為區域中的帳戶部署一致性套件。您也可以編輯和刪除已部署的一致性套件。

## 使用範本部署一致性套件

您可以使用範例範本或您自己的自訂AWS Config範本來部署一致性套件。如需如何建立個人化一致性套件的指示，請參閱自訂一致性套件。

1. 請登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/config/ 的 AWS Config 主控台。
2. 瀏覽至 Conformance packs (一致性套件) 頁面，然後選擇 Deploy conformance pack (部署一致性套件)。
3. 在 Specify template (指定範本) 頁面上，選擇範例範本或使用現有範本。如需詳細資訊，請參閱一致性套件範本。
   - 如果您選擇「使用範例範本」，請從範例範本的下拉式清單中選取範例範本。

     如需每個範本的內容的相關資訊，請參閱一致性套件範例範本。

- 如果您選擇 Template is ready (範本已就緒)，請指定範本來源。它可以是 Amazon S3 URI、AWS Systems Manager文件 (SSM 文件) 或您上傳的範本。

  如果您的範本超過 50 KB，請將其上傳到 S3 儲存貯體，並選取該 S3 儲存貯體位置。例如：s3://*bucketname/prefix*。

  > **Important**
  > 如果您根據「自訂一致性套件」從頭開始建立一致性套件 YAML 檔案，請選擇「範本已準備就緒」。

4. 選擇 下一步。
5. 在 Specify conformance pack details (指定一致性套件詳細資料) 頁面上，輸入一致性套件的名稱。

   一致性套件名稱必須是唯一的名稱，最多可包含 256 個英數字元。名稱可以包含連字號，但不能包含空格。
6. 選用：新增參數。

   參數是在您的範本中定義的，可協助您管理和組織資源。
7. 選擇 下一步。
8. 在 Review and deploy (檢閱和部署) 頁面上，檢閱所有資訊。

   您可以選擇 Edit (編輯) 來編輯範本詳細資訊和一致性套件詳細資訊。
9. 選擇 Deploy conformance pack (部署一致性套件)。

   AWS Config 會在一致性套件頁面上以適當的狀態顯示一致性套件。

   如果一致性套件部署失敗，請檢查您的許可，確認您已完成先決條件步驟，然後再試一次。或者您可以聯繫AWS Support。

若要部署 conformance pack using sample template with remediations (使用具有修補之範例範本的一致性套件)，請先參閱使用一致性套件搭配修補的先決條件，然後使用上述程序。

若要部署具有一或多個AWS Config規則的符合性套件，請參閱。將符合性套件與一或多個規則搭配使用的先決條件 AWS Config

## 編輯一致性套件

1. 若要編輯一致性套件，請從表格中選取一致性套件。
2. 選擇 Actions (動作)，然後選擇 Edit (編輯)。
3. 在 Edit conformance pack (編輯一致性套件) 頁面上，您可以編輯範本詳細資訊、範例範本、一致性套件和參數區段。

   您無法變更一致性套件的名稱。
4. 選擇 Save changes (儲存變更)。

   一致性套件會與 AWS Config 規則一起顯示。

## 刪除一致性套件

1. 若要刪除一致性套件，請從表格中選取一致性套件。
2. 選擇 Actions (動作)，然後選擇 Delete (刪除 VPC)。
3. 在「刪除一####」對話方塊中，確認您是否要永久刪除此一致性套件。

   > **Important**
   >
   > 您無法還原此動作。當您刪除一致性套件時，會同時刪除該一致性套件中的所有 AWS Config 規則和修補動作。

4. 輸入 Delete (刪除) 並選擇 Delete (刪除)。

   在 Conformance packs (一致性套件) 頁面上，您會看到部署狀態顯示為 Deleting (刪除中)，直到一致性套件完全刪除為止。

# 使用 AWS Command Line Interface部署一致性套件

您可以使用 AWS Command Line Interface (AWS CLI) 部署、檢視、更新、檢視 AWS Config 符合性狀態及刪除一致性套件。

AWS CLI 這是一個統一的工具來管理您的 AWS 服務。只要下載和設定一個工具，您就可以從命令列控制多個 AWS 服務，並使用指令碼將它們自動化。若要取得有關 AWS CLI 和安裝 AWS CLI 工具的更多資訊，請參閱《AWS Command Line Interface 使用指南》中的以下內容。

- AWS Command Line Interface 使用者指南
- 設定 AWS Command Line Interface

如有必要，請鍵入`aws configure`以配置 AWS CLI 以使用提供一致性包的「 AWS 區域」。

主題


- 部署一致性套件
- 檢視一致性套件
- 檢視一致性套件狀態
- 檢視一致性套件合規狀態
- 取得特定一致性套件的合規詳細資訊
- 刪除一致性套件


## 部署一致性套件

1. 開啟命令提示或終端機視窗。
2. 鍵入下列其中一項命令以部署名為 **MyConformancePack** 的一致性套件。範本來源可以是 Amazon S3 URI、您上傳的範本或 AWS Systems Manager 文件 (SSM 文件)。

   Amazon S3 URL

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://AmazonS3BucketName/templateName.yaml"
   --delivery-s3-bucket AmazonS3BucketName
   ```

   本機目錄的 YAML 範本

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager 文件 (Systems Manager 文件)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   ```

```
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket AmazonS3BucketName
```

3. 按 Enter 以執行指令。

   您應該會看到類似下列的輸出。

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> 如需有關為一致性套件建立 YAML 範本的詳細資訊，請參閱《自訂一致性套件》。

## 檢視一致性套件

1. 輸入以下命令。

```
aws configservice describe-conformance-packs
```

   或

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. 您應該會看到類似下列的輸出。

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

## 檢視一致性套件狀態

1. 輸入以下命令。

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. 您應該會看到類似下列的輸出。

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

## 檢視一致性套件合規狀態

1. 輸入以下命令。

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. 您應該會看到類似下列的輸出。

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
```

```
        }
    ]
}
```

## 取得特定一致性套件的合規詳細資訊

1. 輸入以下命令。

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. 您應該會看到類似下列的輸出。

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
```

```
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

## 刪除一致性套件

輸入以下命令。

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

若成功的話，命令會在沒有其他輸出的情況下執行。

> **Important**
>
> 您無法還原此動作。當您刪除一致性套件時，您會刪除該合格性套件中的所有 AWS Config 規則與修正動作。

# 管理一致性套件 (API)

使用下列 AWS Config API 動作來管理一致性套件：

- DeleteConformance封裝，刪除指定的一致性套件，以及該合格性套件中的所有 AWS Config 規則與所有評估結果。
- DescribeConformancePackCompliance，會傳回該一致性套件中每個規則的符合性資訊。
- DescribeConformance套件會傳回一或多個符合性套件的清單。
- DescribeConformancePackStatus，提供一或多個符合性套件部署狀態。
- GetConformancePackCompliance詳細資訊，會傳回符合性套件所有 AWS 資源的一致性套件的合規性詳細資訊。
- GetConformancePackCompliance摘要，會根據該符合性套件中所有規則的累計符合性結果，傳回符合性套件的相容性資訊。
- ListConformancePackCompliance分數，傳回一致性套件相容性分數清單。
- PutConformance打包、建立或更新一致性套件。

# 管理組織中所有帳戶的一致性套件

用 AWS Config 於管理組織 AWS 帳戶 內所有人的一致性套件。您可以執行下列作業：

- 在 AWS Organizations中集中部署、更新和刪除組織中所有成員帳戶的一致性套件。
- 在所有帳戶中部署一組通用 AWS Config 規則和修復動作，並指定不應在其中建立 AWS Config 規則和修正動作的帳戶。
- 使用中的管理帳戶 AWS Organizations 來強制執行管理，方法是確保組織的成員帳戶無法修改基礎 AWS Config 規則和補救動作。

## 考量事項

針對跨不同區域的部署

跨帳戶部署規則和一致性套件的 API 呼叫是 AWS 區域特定的。如果您想要在其他區域中部署規則，則必須在組織層級將 API 呼叫的內容變更為不同區域。例如，若要在美國東部 (維吉尼亞北部) 部署規則，請將區域變更為美國東部 (維吉尼亞北部)，然後呼叫 `PutOrganizationConfigRule`。

針對組織內的帳戶

如果有新帳戶加入組織，則會將規則或一致性套件部署至該帳戶。當帳戶離開組織時，會移除規則或一致性套件。

如果您在組織管理員帳戶中部署組織規則或一致性套件，然後建立委派的管理員帳戶，並在委派的管理員帳戶中部署組織規則或一致性套件，您將無法從委派管理員帳戶中查看組織管理員帳戶內的組織規則或一致性套件，或從組織管理員帳戶中查看委派管理員帳戶內的組織規則或一致性套件。DescribeOrganizationConfigRules和 DescribeOrganizationConformancePacksAPI 只能查看從呼叫這些 API 的帳戶內部部署的組織相關資源，並與之互動。

新增至組織之新帳戶的重試機制

如果無法使用記錄器，則只有在帳戶新增至組織後，才會持續 7 小時重試部署現有組織規則和一致性套件。如果在將帳戶新增至組織的 7 小時內不存在記錄器，則應建立記錄器。

組織管理帳戶、委派管理員和服務連結角色

如果您使用組織管理帳戶並打算使用委派的系統管理員進行組織部署，請注意， AWS Config 不會自動建立服務連結角色 (SLR)。您必須使用 IAM 個別手動建立服務連結角色 (SLR)。

如果您的管理帳戶沒有 SLR，您將無法從委派的系統管理員帳戶將資源部署到該帳戶。您仍然可以從管理和委派的管理員帳戶將一致性套件部署至成員帳戶。如需詳細資訊，請參閱 AWS Identity and Access Management (IAM) 使用指南中的使用服務連結角色。

## 部署

To deploy with the AWS Management Console

若要透過 AWS 主控台在整個組織中部署一致性套件，請使用。 AWS Systems Manager如需詳細資訊，請參閱《AWS Systems Manager 使用指AWS Config 南》中的部署一致性套件。

To deploy with the AWS API

若要取得有關如何 AWS Config 與之整合的資訊 AWS Organizations，請參閱《AWS Organizations 使用指南》 AWS Organizations中的AWS Config 和。在您使用下列 API 管理組織內所有相符性套件規則之前，請確定已 AWS 帳戶 開啟 AWS Config 錄製檔：

- DeleteOrganizationConformancePack，刪除指定的組織一致性套件，以及該組織中所有成員帳戶中的所有組態規則與修正動作。
- DescribeOrganizationConformancePacks，會傳回組織一致性套件清單。
- DescribeOrganizationConformancePack狀態，提供組織的組織一致性套件部署狀態。
- GetOrganizationConformancePackDetailedStatus，針對指定的組織一致性套件，傳回組織內每個成員帳戶的詳細狀態。
- PutOrganizationConformancePack」下，跨組織中的成員帳戶部署一致性套件。 AWS

## 區域支援

下列區域支援跨組 AWS 織中的成員帳戶部署一致性套件。

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國西部 (加利佛尼亞北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# 故障診斷

## 符合性套件的失敗狀態

如果您在建立、更新和刪除一致性套件時收到錯誤指出一致性套件失敗，您可以檢查一致性套件的狀態。

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

您應該會看到類似下列的輸出。

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

如需失敗ConformancePackStatusReason的相關資訊，請檢查。

When the stackArn is present in the response (當回應中存在 stackArn 時)

如果錯誤訊息不清楚，或是失敗是由於內部錯誤造成，請移至 AWS CloudFormation 主控台並執行下列動作：

1. 在輸出中搜尋 stackArn。
2. 選擇 CloudFormation 堆疊的 [事件] 索引標籤，並檢查失敗的事件。

   狀態原因指出一致性套件失敗的原因。

When the stackArn is not present in the response (當回應中不存在 stackArn 時)

如果您在建立一致性套件時收到失敗，但 stackArn 不存在於狀態回應中，則可能的原因是堆疊建立失敗並回 CloudFormation 復並刪除堆疊。前往 CloudFormation 主控台並搜尋處於「已刪除」狀態的堆疊。該處可能有提供失敗的堆疊。 CloudFormation 堆疊包含一致性套件名稱。如果您找到失敗的堆疊，請選擇 CloudFormation 堆疊的 [事件] 索引標籤，並檢查失敗的事件。

如果這些步驟都無效，而且失敗原因是內部服務錯誤，請再次嘗試操作或聯絡中AWS Support 心。

## 符合性套件中的懸置規則

部署一致性套件涉及在背景中建立基礎 AWS CloudFormation 堆疊，以便在一致性套件範本中部署規則。這些規則是服務連結規則，無法在一致性套件之外更新或刪除。

如果您對基礎 CloudFormation 堆疊進行變更，這會導致一致性套件及其規則變得無法管理的情況。這些無法管理的規則是懸空的規則。

CloudFormation 堆棧和一致性包之間的漂移

您可以直接從主控台更新一致性套件範本中的規則名稱。 CloudFormation 如果您直接從 CloudFormation 主控台更新範本，則不會更新已部署的一致性套件。

此漂移會建立懸置規則。如果您嘗試從一致性套件刪除規則，您會收到類似下列內容的錯誤訊息：

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

如果您嘗試刪除一致性套件，則無法刪除懸置規則，且您會收到類似下列內容的錯誤訊息：

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

若要修正此問題，請執行下列步驟：

1. 刪除堆疊 如需詳細資訊，請參閱《使用指南》中的〈刪除 AWS CloudFormation 主控台上的堆疊 CloudFormation 〉。
2. 使用 AWS Config 主控台或使用套件 API 刪除一致性DeleteConformance套件。
   如果它是組織一致性套件，且您使用的是管理或委派的管理員帳戶，請使用 DeleteOrganizationConformancePackAPI。
3. 使用符合性包AWS Support 中懸掛規則的 Amazon 資源名稱（ARN）與中心聯繫，以幫助清理您的帳戶。

若要避免此問題，請記住以下最佳做法：

- 切勿對一致性套件的 CloudFormation 堆疊進行任何直接更新。
- 切勿嘗試進行更改，從而在一致性包及其基礎 CloudFormation 堆棧之間造成漂移。
- 無法修改一致性套件的服務連結角色 (SLR)。請確定您要更新的資源是 SLR 權限原則的一部分。

已刪除一致性套件的 CloudFormation 堆疊

除非 CloudFormation 堆棧和一致性包之間存在漂移，否則不建議直接從控制台刪除一致性包或其 CloudFormation 堆棧中的規則。 CloudFormation

若要修正此問題，請使用符合性套件AWS Support 中懸置規則的 Amazon 資源名稱 (ARN) 與中心聯絡，以協助清理您的帳戶。

若要避免此問題，請記住以下最佳做法：

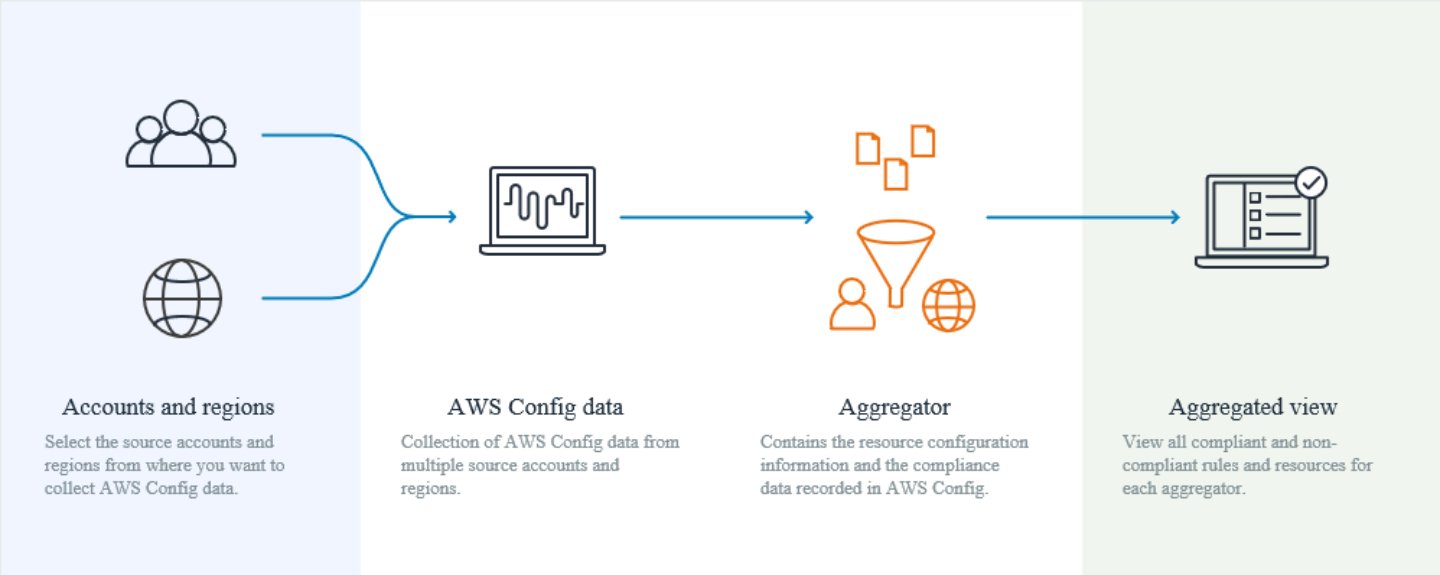
- 切勿刪除一致性套件的基礎 CloudFormation 堆疊。
- 使用套件 API 刪除一致性套件。DeleteConformance如果它是組織一致性套件，且您使用的是管理或委派的管理員帳戶，請使用 DeleteOrganizationConformancePackAPI。

# 多帳戶多區域資料彙整

彙總器是一種 AWS Config 資源類型，可從下列項目收集 AWS Config 組態和符合性資料：

- 多個帳戶和多個 AWS 區域。
- 單一帳戶和多個 AWS 區域。
- 組織中的組織 AWS Organizations 及該組織中已 AWS Config 啟用的所有帳號。

使用彙整工具檢視資源組態和 AWS Config中記錄的合規資料。彙總器使用 Amazon S3 儲存貯體存放彙總資料。它會定期從來源帳戶擷取組態快照，並將其儲存在指定的 S3 儲存貯體中。下圖顯示彙總器如何從多個帳戶和區域收集 AWS Config 資料。




# 使用案例

- 合規監控：您可以彙總合規性資料，以評估組織或跨帳戶和區域的整體合規狀態。
- 變更追蹤：您可以追蹤整個組織的一段時間內，或跨帳戶與區域的資源變更。
- 資源關係：您可以分析整個組織或跨帳戶與區域的資源相依性與關係。

> **Note**
>
> 彙總器透過將來源帳戶中的資料複寫到彙總器帳戶中，提供彙總器授權可檢視的來源帳戶和區域的唯讀檢視。彙總器不提供對來源帳戶或區域的變更存取權。例如，這表示您無法透過彙總器或推播快照檔案透過彙總器將規則部署到來源帳戶或區域。
> 使用彙總工具不會產生任何額外費用。

## 術語

來源帳號是您要彙總 AWS Config 資源組態和符合性資料的來源帳號。 AWS 帳戶 來源帳戶可以是 AWS Organizations中的個別帳戶或組織。您可以個別提供來源帳戶，也可以透過擷取來源帳戶 AWS Organizations。

來源區域是您要彙總 AWS Config 組態與合規性資料的 AWS 地區。

彙總帳戶是您建立彙總工具的帳戶。

授權是指您授與彙總帳戶和區域的權限，以收集您的 AWS Config 組態和合規性資料。如果您要彙整屬於 AWS Organizations一部分的來源帳戶，則不需要授權。

## 如何彙總資料

若要彙總來自來源帳戶和區域的 AWS Config 資料，請從下列項目開始：

1. 新增彙總器以彙總來自多個帳戶和區域的 AWS Config 組態和合規性資料。如需詳細資訊，請參閱 使用主控台設定彙整 及 使用設定彙總器 AWS Command Line Interface。
2. 授權彙總帳戶以收集 AWS Config 組態和合規性資料。如需詳細資訊，請參閱 授權彙總器帳戶使用主控台收集 AWS Config 組態和符合性資料 及 授權彙總帳戶以收集 AWS Config 組態和符合性資料 AWS Command Line Interface。

> **Note**
>
> 彙總工具有兩種類型：個人帳戶彙總工具和組織彙總工具
> 對於個別帳戶彙總工具，任何包含的來源帳戶區域 (包括外部帳戶區域或組織成員帳戶區域) 都需要授權。
> 對於組織彙總者而言，組織成員帳戶區域不需要授權，因為授權已與「組 Organizations」服務整合。

3. 在彙整檢視中監控規則和帳戶的合規資料。如需詳細資訊，請參閱 在彙總工具儀表板中檢視合規與庫存資料。

# 區域支援

目前，下列區域支援多帳戶多區域資料彙總：

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| 美國西部 (加州北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| 非洲 (開普敦) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| 亞太區域 (香港) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| 亞太區域 (海德拉巴) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| 亞太區域 (大阪) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 加拿大西部 (卡加利) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (米蘭) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (西班牙) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 歐洲 (蘇黎世) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| 以色列 (特拉維夫) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| 中東 (巴林) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| 中東 (阿拉伯聯合大公國) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 | |
|---|---|---|---|---|
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS | |

# 多帳戶多區域資料彙整故障診斷

AWS Config 可能無法從來源帳戶彙總資料，原因如下：

| 若發生這種情況 | 執行此作業 |
|---|---|
| AWS Config 未在「組織」中的帳戶的來源帳戶中啟用。 | AWS Config 在來源帳戶中啟用，並授權彙總帳戶收集資料。 |
| 授權並未授予彙整工具帳戶。 | 登入來源帳戶，並授予彙總帳戶以收集 AWS Config 資料的授權。 |
| 可能發生暫時性的問題，防止資料彙整。 | 資料彙整可能有所延遲。請等待數分鐘。 |

AWS Config 可能因為下列其中一個原因而無法彙總組織的資料：

| 若發生這種情況 | 執行此作業 |
|---|---|
| AWS Config 由於無效的 IAM 角色，因此無法存取您的組織詳細資料。 | 建立 IAM 角色，或從 IAM 角色清單選取有效的 IAM 角色。<br><br>**Note**<br>如果 IAM 角色無效超過 24 小時，請 AWS Config 刪除整個組織的資料。 |
| AWS Config 您的組織中已停用服務存取。 | 您可以啟用 API 之間 AWS Config 和 AWS Organizations 透過 `EnableAWSServiceAccess` API 的整合。 |

| 若發生這種情況 | 執行此作業 |
| --- | --- |
| | 如果您選擇 [在主控台中新增我的組織]，AWS Config 會自動啟用 AWS Config 和之間的整合 AWS Organizations。 |
| AWS Config 無法存取您的組織詳細資料，因為您的組織未啟用所有功能。 | 啟用 AWS Organizations 主控台中的所有功能。 |
| 中東 (巴林) 和亞太區域 (香港) 區域不會立即更新新增帳戶、移除帳戶、啟用服務存取權及停用服務存取權等組織變更。 | 組織變更可能會延遲 2 小時。等待 2 小時即可查看所有組織變更。 |

# 在彙總工具儀表板中檢視合規與庫存資料

[彙總器] 頁面上的儀表板會顯示彙總 AWS 資源的組態資料。其提供規則、一致性套件及其合規狀態的概觀。

儀表板提供資源的總資 AWS 源計數。資源類型和來源帳戶的排名是根據最高數量的資源。其也會提供合規及不合規規則與一致性套件的計數。不合規規則的排名是根據最高數量的不合規資源。不合規一致性套件與來源帳戶的排名是根據最高數量的不合規規則。

設定完成後 AWS Config，會開始將指定來源帳戶的資料彙總至彙總器。可能需要數分鐘才會顯示規則的合規狀態。

## 使用彙總工具儀板表

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 導覽到 彙總工具 頁面。您可以檢視：
   - 您的規則及其合規狀態。
   - 您的一致性套件及其合規狀態。
   - 您的 AWS 資源及其組態資料。
3. 從儀表板選擇彙總工具。依彙總工具名稱篩選彙總工具。您可以檢視下列小工具：
   - 資源庫存

檢視所選彙總工具中前 10 個資源類型 (根據資源計數以遞減順序列出)。選擇所選彙總工具的資源總數 (顯示在 資源庫存 後面的括號中)，即可移至彙總的 資源 頁面，您可以在此頁面中檢視彙總工具的所有資源。或者，在小工具中選擇資源類型以移至彙總的資源頁面，並使用指定的資源類型進行篩選。

- 依資源計數列出的帳戶

  檢視所選彙總工具中前五個帳戶 (根據資源計數以遞減順序列出)。在小工具中選擇帳戶以移至資源 頁面，並使用指定的帳戶進行篩選。

- 不合規規則

  檢視所選彙總工具中前五個不合規規則 (根據不合規資源的數目以遞減順序列出)。在小工具中選擇規則，以移至指定規則的詳細資訊頁面。選擇 檢視所有不合規規則，即可移至彙總的 規則 頁面，您可以在此頁面中檢視彙總工具的所有規則。

- 依不合規規則列出的帳戶

  檢視所選彙總工具中前五個帳戶 (根據不合規規則的數目以遞減順序列出)。在小工具中選擇一個帳戶，即可移至彙總的 規則 頁面，您可以在此頁面中檢視使用指定帳戶篩選之彙總工具的所有規則。

- 依不合規一致性套件列出的帳戶

  檢視所選彙總工具中前五個帳戶 (根據不合規一致性套件的數目以遞減順序列出)。在小工具中選擇一個帳戶，即可移至彙總的 一致性套件 頁面，您可以在此頁面中檢視使用指定帳戶篩選之彙總工具的所有一致性套件。

4. 在左側導覽窗格中，從下拉式功能表選擇下列其中一個選項：

- 合規儀表板

  使用可總結彙總工具內資源合規性洞察的小工具，以檢視自動化合規儀表板。您可以查看依不合規資源列出的前 10 個資源類型，以及依不合規規則列出的前 10 個帳戶層級一致性套件等資料。如需這些圖形和圖表的資訊，請參閱《合規儀表板》。

- 一致性套件

  檢視在聚合器 AWS 帳戶 中建立並連結至其他標準套件的所有一致性套件。一致性套件頁面會顯示一個資料表，其中列出每個一致性套件的名稱、區域、帳戶 ID 及合規狀態。您可以從此頁面選擇一致性套件和 檢視詳細資訊，以取得有關其規則、資源及其合規狀態的詳細資訊。

- 規則

檢視彙總工具內已建立並連結至不同 AWS 帳戶的所有規則。規則頁面會顯示一個資料表，其中列出每個規則的名稱、合規狀態、區域及帳戶。您可以從此頁面選擇規則和 檢視詳細資訊，以取得其彙總工具、區域、帳戶 ID 及範圍內的資源等資訊。

- 庫存儀表板

  使用可總結彙總工具內資源組態資料洞察的小工具，以檢視自動化庫存儀表板。您可以查看依資源計數列出的前 10 個資源類型，以及依資源計數列出的前 10 個帳戶等資料。如需這些圖形和圖表的資訊，請參閱《庫存儀表板》。

- 資源

  檢視彙總工具內已記錄並連結至不同 AWS 帳戶的所有資源。從資源頁面中選擇資源和 檢視詳細資訊，以檢視其詳細資訊、與其相關聯的規則及目前的資源組態。您也可以查看資源的相關資訊，例如其彙總工具、區域、帳戶 ID、資源名稱、資源類型及資源 ID。

- 授權

  檢視並管理目前授權或待授權的所有帳戶。從 授權 頁面中，選擇 新增授權 以提供對其他帳戶的存取權。選擇 刪除授權 以撤銷帳戶 ID 的存取權。

> **Note**
>
> 疑難排解
>
> 您可能會看到彙總檢視由於下列原因顯示 從所有來源帳戶及區域進行的資料收集未完成 訊息：
>
> - 不符合標準的規 AWS Config 則和 AWS 資源的組態資料的傳輸正在進行中。
> - AWS Config 找不到符合您套用之篩選條件的規則。選取適當的帳戶或區域，然後再試一次。
>
> 您可能會看到彙總檢視中顯示此訊息：從所有來源帳戶及區域進行的資料收集未完成。您只能在 24 小時內檢視以下資料。其顯示的原因如下：
>
> - AWS Config 無法存取您的組織詳細資料，因為 IAM 角色無效。若 IAM 角色無效時間超過 24 小時，則 AWS Config 會刪除整個組織的資料。
> - AWS Config 您的組織中已停用服務存取。

# 合規儀表板

使用可總結彙總工具內資源合規性洞察的小工具，以檢視自動化合規儀表板。此儀表板只會顯示具有合規結果的規則。

> **Note**
>
> 限制
>
> 符合性儀表板中的深入解析是由的「進階查詢」功能提供 AWS Config，而且此功能不支援巢狀結構或解壓縮巢狀陣列。這表示符合性儀表板會顯示資源的整體符合性，而不是針對資源報告的每個特定規則顯示符合性狀態。
>
> 例如，如果您檢查資源類型的配置項目 (CI)`AWS::Config::ResourceCompliance`，儀表板將顯示報告該資源的所有規則的符合性結果。如果在資源上報告有 10 個規則，其中 9 個是「相容」，而且只有 1 個是「不符合 _ 標準」，則該資源的整體符合性將為「不符合 _ 標準」。

依資源劃分的合規摘要

顯示圓餅圖，比較所選聚總器中相容資源與不相容資源的數目。將滑鼠游標暫留在圖表上，即可查看相容和不符合資源的確切數目和百分比。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

依不相容資源分類的前 10 種資源類型

顯示水平長條圖，比較所選聚總器中最多 10 個資源類型 (依不相容資源數目遞減順序)。將游標暫留在圖形上，即可查看每個資源類型的不相容資源的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

依不相容資源分類的前 10 個帳號

依不相容資源排列的前 10 個帳號會顯示一個水平長條圖，比較所選聚總工具中最多 10 個帳號 (依不相容資源的數目遞減順序)。將滑鼠游標暫留在圖表上，即可查看每個帳號的不相容資源的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

依不相容資源排名的前 10 個區域

顯示比較最多 10 個區域的水平長條圖，其中選取的聚總器會依不相容資源的數目遞減順序收集資料。將滑鼠游標暫留在圖表上，即可查看每個區域的確切不相容資源數量。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定。

依不相容規則分類的前 10 個帳戶層級一致性套件

顯示水平長條圖，比較所選彙總器中最多 10 個帳戶層級一致性套件 (依不相容規則數目遞減順序)。將滑鼠游標暫留在圖表上，即可查看每個帳戶層級一致性套件的合規與不合規規則百分比。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

依不相容規則分類的前 10 個組織層級符合性套件

顯示水平長條圖，比較所選聚總器中最多 10 個組織層級一致性套件 (依不相容規則數目遞減順序)。將滑鼠游標暫留在圖形上，即可查看每個組織層級一致性套件中相容與不相容規則的百分比。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

依符合性套件中不相容規則排列的前 10 個帳號

各合格套件中不相容規則排列的前 10 名帳戶會顯示一個水平長條圖，比較所選聚總器中最多 10 個帳戶 (依所有符合性套件中不相容規則的數目遞減順序)。將滑鼠游標暫留在圖表上，即可查看每個帳戶中不符合規則的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

## 庫存儀表板

使用可總結彙總工具內資源組態資料洞察的小工具，以檢視自動化庫存儀表板。

依資源計數列出的前 10 個資源類型

顯示的水平長條圖可比較所選彙總工具中多達 10 個資源類型 (根據資源計數以遞減順序列出)。將滑鼠游標移至圖表上方，即可查看每個資源類型中資源的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

依區域劃分的資源計數

顯示的水平長條圖可比較所選彙總工具在其中收集資料的區域，數量多達 10 個 (根據資源計數以遞減順序列出)。將滑鼠游標移至圖表上方，即可查看每個區域中資源的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定。

依資源計數列出的前 10 個帳戶

顯示的水平長條圖可比較所選彙總工具中多達 10 個帳戶 (根據資源計數以遞減順序列出)。將滑鼠游標移至圖表上方，即可查看每個資源類型中資源的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。

依 Amazon EC2 服務資源類型劃分的資源計數

顯示的水平長條圖可比較所選彙總工具中的 Amazon EC2 資源類型 (根據資源計數以遞減順序列出)。將滑鼠游標移至圖表上方，即可查看每個 Amazon EC2 資源類型中資源的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。若要使用此圖表，您必須設定記錄器以記錄 Amazon EC2 資源類型。如需詳細資訊，請參閱選取哪些資源 AWS Config 記錄。

使用的前 10 個 EC2 執行個體類型

顯示的水平長條圖可比較所選彙總工具中多達 10 個 Amazon EC2 執行個體類型 (根據用量以遞減順序列出)。將滑鼠游標移至圖表上方，即可查看每個 EC2 執行個體類型的用量。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。若要使用此圖表，您必須設定記錄器以記錄 EC2 執行個體資源類型。如需詳細資訊，請參閱重新編碼 AWS 資源。

按磁碟區類型和大小的 EBS 磁碟區計數

顯示的垂直長條圖可根據資源計數，比較所選彙總工具中的 EBS 磁碟區。將滑鼠游標移至圖表上方，即可查看每種 EBS 磁碟區類型的計數和大小明細。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。若要使用此圖表，您必須設定記錄器以記錄 EC2 磁碟區資源類型。如需詳細資訊，請參閱選取哪些資源 AWS Config 記錄。

依類型劃分的執行中與已停止的 EC2 執行個體數目

顯示的水平長條圖可根據執行個體類型，比較所選彙總工具中執行中的 EC2 執行個體類型與已停止的 EC2 執行個體。將滑鼠游標移至圖表上方，即可查看每種類型中已停止與執行中 EC2 執行個體的確切數目。

顯示的資料取決於所選彙總工具中每個帳戶的組態記錄器設定，以及所選彙總工具設定為收集資料的區域。若要使用此圖表，您必須設定記錄器以記錄 EC2 執行個體資源類型。如需詳細資訊，請參閱重新編碼 AWS 資源。

# 使用主控台設定彙整

在 Aggregator (彙整) 頁面上，您可以執行下列動作。

- 透過指定來源帳戶 ID 或組織，或是您希望彙整資料的區域，建立彙整。
- 編輯及刪除彙整。

主題


- 建立彙整工具
- 編輯彙整工具
- 刪除彙整工具


## 建立彙整工具

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 導覽至 彙整工具 頁面，並選擇 建立彙總工具。
3. 允許數據複製，授 AWS Config 予將數據從源帳戶複製到聚合器帳戶的權限。

   選擇 [ AWS Config 允許] 將來源帳戶中的資料複製到彙總帳戶。您必須選取此核取方塊才能繼續新增彙總工具。
4. 針對 Aggregator name (彙整工具名稱)，輸入彙整工具的名稱。

   彙整工具名稱必須是最多 64 個英數字元的唯一名稱。名稱可以包含連字號和底線。
5. 針對 Select source accounts (選取來源帳戶)，選擇 Add individual account IDs (新增個別帳戶 ID) 或 Add my organization (新增我的組織)，以從中彙總資料。

> **Note**
>
> 使用 新增個別帳戶 ID 以選取來源帳戶時，需要授權。

- 如果您選擇 Add individual account IDs (新增個別帳戶 ID)，則可以新增彙整工具帳戶的個別帳戶 ID。
  1. 選擇 Add source accounts (新增來源帳戶) 來新增帳戶 ID。
  2. 選擇「新增 AWS 帳戶 ID」以手動新增逗號分隔的 AWS 帳戶 ID。如果您要彙整目前帳戶中的資料，請輸入帳戶的帳戶 ID。

     或

     選擇「上傳檔案」以上傳以逗 AWS 帳戶 號分隔 ID 的檔案 (.txt 或 .csv)。
  3. 選擇 Add source accounts (新增來源帳戶)，確認您選取的項目。
- 如果您選擇 Add my organization (新增我的組織)，則可以將組織中的所有帳戶都新增至彙整工具帳戶。

> **Note**
>
> 您必須先登入管理帳戶或註冊委派管理員，且啟用組織中的所有功能。如果來 AWS Config 電者是管理帳戶，請呼叫 `EnableAwsServiceAccess` API 以啟用 AWS Config 和之間的整合 AWS Organizations。如果呼叫者是已註冊的委派管理員，請 AWS Config 呼叫 `ListDelegatedAdministrators` API 以驗證呼叫者是否為有效的委派管理員。
> 請確定管理帳戶在委派的系統管理員建立彙總器之前，已為 AWS Config 服務主體名稱 (config.amazonaws.com) 註冊委派的管理員。若要註冊委派管理員，請參閱《註冊委派管理員》。

您必須指派 IAM 角色， AWS Config 才能為組織呼叫唯讀 API。

1. 選擇 從您的帳戶選擇角色 以選取現有 IAM 角色。

> **Note**
>
> 在 IAM 主控台中，將 `AWSConfigRoleForOrganizations` 受管政策連接至您的 IAM 角色。附加此原則可 AWS Config 讓您呼叫 AWS Organizations `DescribeOrganizationListAWSServiceAccessForOrganization`、和 `ListAccounts` API。`config.amazonaws.com` 預設會自動指定為受信任的實體。

2. 或者，選擇 建立角色，然後鍵入 IAM 角色名稱的名稱，以建立 IAM 角色。

6. 針對 Regions (區域)，選擇您要彙整資料的區域。
   - 選擇一或多個區域，或所有 AWS 區域。
   - 選取「包含 future」 AWS 區域以彙總所有已啟用多帳戶多區域資料彙總的 future 資料。 AWS 區域
7. 選擇 [儲存]。 AWS Config 顯示聚合器。

## 編輯彙整工具

1. 若要變更彙整工具，請選擇彙整工具名稱。
2. 選擇 Actions (動作)，然後選擇 Edit (編輯)。
3. 使用 編輯彙整工具 頁面上的各區段，以變更彙整工具的來源帳戶、IAM 角色或區域。

> **Note**
>
> 您無法將個別帳戶的來源類型變更為組織，反之亦然。

4. 選擇儲存。

## 刪除彙整工具

1. 若要刪除彙整工具，請選擇彙整工具名稱。
2. 選擇 Actions (動作)，然後選擇 Delete (刪除 VPC)。

   即會顯示警告訊息。刪除彙整工具會遺失所有彙整資料。您無法復原此資料，但來源帳戶中的資料不會受到影響。

3. 選擇 Delete (刪除) 確認您選取的項目。

# 使用設定彙總器 AWS Command Line Interface

您可以使用 () 建立、檢視、更新和刪除 AWS Config 彙總資 AWS Command Line Interface AWS CLI 料。

AWS CLI 這是一個統一的工具來管理您的 AWS 服務。只要下載和設定一個工具，您就可以從命令列控制多個 AWS 服務，並使用指令碼將它們自動化。若要取得有關 AWS CLI 和安裝 AWS CLI 工具的更多資訊，請參閱《AWS Command Line Interface 使用指南》中的以下內容。

- AWS Command Line Interface 使用者指南
- 設定 AWS Command Line Interface

如有必要，請輸入`aws configure`以配置 AWS CLI 以使用可用彙總工具的「 AWS 區域」。

主題


- 使用個別帳戶新增彙整
- 使用 AWS Organizations 新增彙整工具
- 註冊委派管理員
- 檢視彙整
- 編輯彙整工具
- 刪除彙整工具


## 使用個別帳戶新增彙整

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，建立名為 **MyAggregator** 的彙整工具。

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

針對 `account-aggregation-sources`，輸入下列其中之一：

- 您要彙總資料的 AWS 帳戶 ID 清單 (以逗號分隔)。以方括弧包圍帳戶 ID，並確認逸出雙引號 (例如，`"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`)。
- 您也可以上傳以逗號分隔 AWS 帳戶 ID 的 JSON 檔案。使用下列語法上傳檔案：`--account-aggregation-sources MyFilePath/MyFile.json`

  JSON 檔案必須採用下列格式：

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. 按 Enter 以執行命令。

   您應該會看到類似下列的輸出：

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
```

```
    }
}
```

## 使用 AWS Organizations 新增彙整工具

您必須先登入管理帳戶或註冊委派管理員，並啟用您組織中的所有功能，才能開始此程序。

> **Note**
>
> 在委派的管理員建立彙總器之前，請確定管理帳戶已使用下列兩個 AWS Config 服務主體名稱 (`config.amazonaws.com`和`config-multiaccountsetup.amazonaws.com`) 註冊委派的管理員。若要註冊委派管理員，請參閱《註冊委派管理員》。

1. 開啟命令提示或終端機視窗。
2. 如果尚未為 AWS Config 彙總器建立 IAM 角色，請輸入下列命令：

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> 從這個 IAM 角色複製 Amazon 資源名稱 (ARN)，以便在建立 AWS Config 彙總工具時使用。您可以在回應物件中找到 ARN。

3. 如果尚未將政策附加到 IAM 角色，請附加受AWSConfigRoleForOrganizations管政策或輸入以下命令：

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAWSSe
```

4. 輸入下列命令，建立名為 **`MyAggregator`** 的彙整工具。

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. 按 Enter 以執行命令。

   您應該會看到類似下列的輸出：

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

## 註冊委派管理員

委派管理員是指定「 AWS 組織」內的帳戶，這些帳戶被授與指定 AWS 服務的其他管理權限。

1. 使用管理帳戶憑證登入。
2. 開啟命令提示或終端機視窗。
3. 輸入下列命令，以委派管理員身分啟用服務存取，讓您的組織在整個組織中部署及管理 AWS Config 規則與一致性套件：

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. 輸入下列命令，以委派管理員身分啟用服務存取權，讓您的組織彙總整個組織的 AWS Config 資料：

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. 若要檢查是否已完成服務存取權啟用，請輸入下列命令，然後按 Enter 以執行指令。

```
aws organizations list-aws-service-access-for-organization
```

您應該會看到類似下列的輸出：

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. 接下來，請輸入下列命令將成員帳戶註冊為 AWS Config的委派管理員。

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

以及

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. 若要檢查是否已完成委派管理員註冊，請從管理帳戶輸入下列命令，然後按 Enter 以執行命令。

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

以及

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

您應該會看到類似下列的輸出：

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::MemberAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

## 檢視彙整

1. 輸入以下命令：

```
aws configservice describe-configuration-aggregators
```

2. 根據您的來源帳戶，您應該會看到與下列內容相似的輸出：

針對個別帳戶

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
```

```
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

或

針對組織

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

## 編輯彙整工具

1. 您可以使用 `put-configuration-aggregator` 命令更新或編輯組態彙整。

   輸入下列命令，將新的帳戶 ID 新增至 **MyAggregator**：

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

2. 根據您的來源帳戶，您應該會看到與下列內容相似的輸出：

針對個別帳戶

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

或

針對組織

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
```

```
}
```

## 刪除彙整工具

輸入以下命令：

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

若成功的話，命令會在沒有其他輸出的情況下執行。

# 授權彙總器帳戶使用主控台收集 AWS Config 組態和符合性資料

AWS Config 可讓您授權帳戶收集 AWS Config 組態和符合性資料。

在 Authorizations (授權) 頁面上，您可以執行下列作業：

- 新增授權以允許指定彙總工具帳戶及區域從您現有帳戶收集 AWS Config 組態和合規資料。
- 授權來自彙總工具帳戶的待定請求，以收集您目前帳戶的 AWS Config 組態和合規資料。
- 刪除彙總工具帳戶的授權，即可從您目前的帳戶收集 AWS Config 組態和合規資料。

主題


- 考量事項
- 新增彙整工具帳戶及區域的授權
- 授權彙整工具帳戶的擱置中請求
- 刪除現有彙總工具帳戶的授權


## 考量事項

彙總工具有兩種類型：個人帳戶彙總工具和組織彙總工具

針對個別帳戶彙總工具，您想要包含的所有來源帳戶與區域都需要授權，包括外部帳戶與區域，以及組織成員帳戶與區域。

對於組織彙總者，組織成員帳戶區域不需要授權，因為授權已與 AWS Organizations 服務整合。

彙總工具不會代表您自動 AWS Config 啟用

AWS Config 需要在來源帳戶和區域中針對任一類型的彙總器啟用，才能在來源帳戶和區域中產生 AWS Config 資料。

## 新增彙整工具帳戶及區域的授權

您可以新增授權，以授與彙總帳戶和區域收集 AWS Config 組態和符合性資料的權限。

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 導覽至 Authorizations (授權) 頁面，然後選擇 Add authorization (新增授權)。
3. 針對 Aggregator account (彙整工具帳戶)，輸入彙整工具帳戶的 12 位數帳戶 ID。
4. AWS 區域 在「彙總器」區域中，選擇允許彙總帳戶收集 AWS Config 組態和合規性資料的位置。
5. 選擇 Add authorization (新增授權)，確認您選取的項目。

   AWS Config 顯示彙總帳戶、地區和授權狀態。

> **Note**
>
> 您也可以使 AWS CloudFormation 用範例範本以程式設計方式將授權新增至彙總帳戶和區域。若要取得更多資訊，請參閱《AWS CloudFormation 使用指南》AWS::Config::AggregationAuthorization中的。

## 授權彙整工具帳戶的擱置中請求

若您有來自現有彙總工具帳戶的待定授權請求，您會在 授權 頁面看到請求狀態。您可以從此頁面授權擱置中請求。

1. 選擇您要授權的彙總工具帳戶，然後選擇 授權。

   此時會顯示確認訊息，確認您要授與彙總帳戶從此帳戶收集 AWS Config 資料的權限。
2. 再次選擇 授權 以確認您要將許可授與彙總工具帳戶。

   授權狀態會從 Requesting for authorization (請求授權中) 變更為 Authorized (已授權)。

授權核准期限

若要將來源帳戶新增至個別帳戶彙總工具，則需要獲得授權核准。將來源帳戶新增至個別帳戶彙總工具後，待定的授權核准申請將在 7 天內有效。

## 刪除現有彙總工具帳戶的授權

1. 選擇您希望刪除授權的彙總工具帳戶，並選擇 刪除。

   即會顯示警告訊息。當您刪除此授權時， AWS Config 資料將不再與彙總帳戶共用。

2. 再次選擇 刪除 以確認您選取的項目。

   現已刪除彙總工具帳戶。

在刪除彙整工具的授權之後，資料會留在彙整工具帳戶中最多 24 個小時，之後便會刪除。

# 授權彙總帳戶以收集 AWS Config 組態和符合性資料 AWS Command Line Interface

您可以使用 AWS Command Line Interface (AWS CLI) 授權彙總帳戶從來源帳戶收集 AWS Config 資料，並刪除彙總帳戶。若要使用 AWS 管理主控台，請參閱授權彙總器帳戶使用主控台收集 AWS Config 組態和符合性資料。

AWS CLI 這是一個統一的工具來管理您的 AWS 服務。只要下載和設定一個工具，您就可以從命令列控制多個 AWS 服務，並使用指令碼將它們自動化。若要取得有關 AWS CLI 和安裝 AWS CLI 工具的更多資訊，請參閱《AWS Command Line Interface 使用指南》中的以下內容。

- AWS Command Line Interface 使用者指南
- 設定 AWS Command Line Interface

如有必要，請鍵入`aws configure`以配置 AWS CLI 以使用提供一 AWS Config 致性套件的「 AWS 區域」。

主題


- 考量事項
- 新增彙整工具帳戶及區域的授權
- 刪除授權帳戶

## 考量事項

彙總工具有兩種類型：個人帳戶彙總工具和組織彙總工具

針對個別帳戶彙總工具，您想要包含的所有來源帳戶與區域都需要授權，包括外部帳戶與區域，以及組織成員帳戶與區域。

對於組織彙總者，組織成員帳戶區域不需要授權，因為授權已與 AWS Organizations 服務整合。

彙總工具不會代表您自動 AWS Config 啟用

AWS Config 需要在來源帳戶和區域中針對任一類型的彙總器啟用，才能在來源帳戶和區域中產生 AWS Config 資料。

## 新增彙整工具帳戶及區域的授權

1. 開啟命令提示或終端機視窗。
2. 輸入以下命令：

```
aws configservice put-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

3. 您應該會看到類似下列的輸出：

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

## 刪除授權帳戶

輸入以下命令：

```
aws configservice delete-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

若成功的話，命令會在沒有其他輸出的情況下執行。

# 查詢 AWS 資源目前的組態狀態

介紹進階查詢的預覽功能，可讓您使用生成人工智慧 (生成 AI) 功能以純英文輸入提示，並將其轉換為 ready-to-use 查詢格式。如需詳細資訊，請參閱進階查詢的自然語言查詢處理器。

您可以使 AWS Config 用根據單一帳戶和區域或跨多個帳戶和區域的組態屬性來查詢 AWS 資源的目前組態狀態。您可以跨支援的資源清單，針對目前的 AWS 資源狀態中繼資料執行屬性型查詢。 AWS Config 如需所支援資源類型清單的詳細資訊，請參閱《進階查詢支援的資源類型》。

進階查詢提供單一查詢端點和查詢語言，以取得目前的資源狀態中繼資料，而無需執行服務特定的描述 API 呼叫。您可以使用組態彙總工具，從中央帳戶跨多個帳戶和 AWS 區域執行相同的查詢。

主題


- 功能
- 查詢元件
- 查詢範例
- 範例關係查詢
- 限制
- 區域支援
- 使用 SQL 查詢編輯器 (主控台) 查詢
- 使用 SQL 查詢編輯器 (AWS CLI) 進行查詢
- 進階查詢的自然語言查詢處理器


## 功能

AWS Config 使用結構化查詢語言 (SQL) `SELECT` 語法的子集，對目前的設定項目 (CI) 資料執行以屬性為基礎的查詢和彙總。查詢的複雜性範圍從標籤和/或資源識別碼的比對，到更複雜的查詢，例如檢視所有已停用版本控制的 Amazon S3 儲存貯體。這能讓您不需要執行 AWS 服務特定 API 呼叫，即可查詢所需的目前資源狀態。

它支援 `AVG`、`COUNT`、`MAX`、`MIN` 和 `SUM` 等彙總函數。

您可以將進階查詢用於：

- 庫存管理 (例如：擷取特定大小的 Amazon EC2 執行個體清單)。
- 安全性和營運情報 (例如，擷取啟用或停用特定組態屬性的資源清單)。
- 成本最佳化 (例如，識別未連接到任何 EC2 執行個體的 Amazon EBS 磁碟區清單)。
- 合規資料；例如，擷取所有一致性套件及其合規狀態的清單。

如需如何使用 AWS SQL 查詢語言的詳細資訊，請參閱何謂 SQL (結構化查詢語言)？ 。

# 查詢元件

SQL SELECT 查詢元素如以下所示。

## 概要

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

## 參數

[ WHERE condition ]

根據您指定的 `condition` 篩選結果。

[GROUP BY 屬性]

將結果集彙總成資料列群組，並加上特定屬性的符合值。

該組 BY 子句適用於聚合。

[ ORDER BY 屬性 [ ASC | DESC ] [, 屬性 [ ASC | DESC ] ...] ]

依一或多個輸出 `properties` 排序結果集。

當子句包含多個屬性時，結果集會根據第一個 `property` 排序，再將值符合第一個屬性的資料列根據第二個 `property` 排序，以此類推。

## 範例

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

# 查詢範例

Query to list all EC2 instances with AMI ID 阿美

查詢：

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

結果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
```

```
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

查詢：

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

結果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

查詢：

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

結果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
```

```
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

查詢：

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

結果：

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
```

```
}
```

Query to list all EC2 volumes that are not in use

查詢：

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

結果：

```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
```

```
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

# 範例關係查詢

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

或

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

# 限制

> **Note**
>
> 進階查詢不支援尚未設定為由組態記錄程式記錄的查詢資源。 AWS Config 當發現資源但未配置為由組態記錄程式記錄`configurationItemStatus`時，會`ResourceNotRecorded`在中建立配置項目 (CI)。雖然彙總工具會彙總這些 CI，但進階查詢不支援查詢具有 `ResourceNotRecorded` 的 CI。請更新您的記錄器設定，以啟用要查詢之資源類型的記錄。

做為 SQL `SELECT` 的子集，其查詢語法有下列限制：

- 查詢中不支援 ALL、AS、DISTINCT、FROM、HAVING、JOIN 和 UNION 關鍵字。不支援 NULL 值查詢。
- 不支援查詢第三方資源。使用進階查詢擷取的第三方資源，會將組態欄位設定為 NULL。
- 不支援使用 SQL 查詢解壓縮的巢狀結構 (例如標籤)。
- CIDR 標記法會轉換為 IP 範圍以供搜尋。這意味著 "=" 和 "BETWEEN" 會搜尋包含所提供 IP 的任何範圍，而不是確切的 IP。若要搜尋確切的 IP 範圍，您需要新增其他條件以排除範圍以外的 IP。例如，若要搜尋 10.0.0.0/24 並且只搜尋該 IP 區塊，您可以執行下列動作：

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

對於 192.168.0.2/32，您可以使用類似的方式進行搜尋：

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

- 在物件陣列中查詢多種屬性時，系統會針對所有陣列元素進行比對。例如，對於具有規則 A 和 B 的資源 R，資源符合規則 A，但不符合規則 B。則資源 R 儲存為：

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R 將通過下列查詢傳回：

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

第一個條件適用`configuration.configRuleList.complianceType = 'non_compliant'`於 R.config 中的所有元素RuleList，因為 R 具有符合性類型 = '不符合' 的規則（規則 B），因此條件評估為真。第二個條件適用`configuration.configRuleList.configRuleName`於 R.config 中的所有元素RuleList，因為 R 具有 configRuleName = 'A' 的規則（規則 A），條件評估為真。由於這兩個條件都為 True，R 將被傳回。

- SELECT 所有欄位速記 (也就是 `SELECT *`) 只會選取 CI 最上層的純量屬性。傳回的純量屬性為 `accountId`、`awsRegion`、`arn`、`availabilityZone`、`configurationItemCaptureTime`、`resou` 和 `version`。
- 萬用字元限制：
  - 只支援對屬性值使用萬用字元，對屬性金鑰不支援 (例如：支援 `...WHERE someKey LIKE 'someValue%'`，但不支援 `...WHERE 'someKey%' LIKE 'someValue%'`)。
  - 僅支援尾碼萬用字元 (例如：支援 `...LIKE 'AWS::EC2::%'` 和 `...LIKE 'AWS::EC2::_'`，但不支援 `...LIKE '%::EC2::Instance'` 和 `...LIKE '_::EC2::Instance'`)。
  - 萬用字元符合項目的長度必須至少為三個字元 (例如，允許 `...LIKE 'abc%'` 和 `...LIKE 'abc_'`，但不允許 `...LIKE 'ab%'` 和 `...LIKE 'ab_'`)。

> **Note**
>
> 系統也會將 "_" (單底線) 視為萬用字元。

- 彙總限制：
  - 彙總函數只能接受單一引數或屬性。
  - 彙總函數無法將其他函數視為引數。
  - 具有 `ORDER BY` 子句 (參考彙總函數) 的 `GROUP BY`，可能只包含單一屬性。
  - 所有其他彙總 `GROUP BY` 子句可以最多包含三個屬性。
  - 除非 `ORDER BY` 子句具有彙總函數，否則所有彙總查詢都支援分頁功能。例如，如果 Y 是彙總函數，則 `GROUP BY X, ORDER BY Y` 沒有作用。
  - 彙總不支援 `HAVING` 子句。
- 不相符的識別符限制：

不相符的識別符是具有相同拼字，但大小寫不同的屬性。進階查詢不支援處理包含不相符識別符的查詢。例如：

- 兩個屬性具有完全相同的拼字，但具有不同的大小寫 (`configuration.dbclusterIdentifier` 和 `configuration.dBClusterIdentifier`)。
- 兩個屬性，其中一個屬性是另一個屬性的子集，並且具有不同的大小寫 (`configuration.ipAddress` 和 `configuration.ipaddressPermissions`)。

# 區域支援

下列區域支援進階查詢：

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (俄亥俄) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| 美國西部 (加州北部) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| 非洲 (開普敦) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| 亞太區域 (香港) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| 亞太區域 (海德拉巴) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 亞太區域 (雅加達) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| 亞太區域 (墨爾本) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| 亞太區域 (孟買) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| 亞太區域 (大阪) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| 亞太區域 (首爾) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| 亞太區域 (新加坡) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| 亞太區域 (雪梨) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| 亞太區域 (東京) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| 加拿大 (中部) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| 加拿大西部 (卡加利) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| 歐洲 (法蘭克福) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 歐洲 (愛爾蘭) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| 歐洲 (倫敦) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| 歐洲 (米蘭) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| 歐洲 (巴黎) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| 歐洲 (西班牙) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| 歐洲 (斯德哥爾摩) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| 歐洲 (蘇黎世) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| 以色列 (特拉維夫) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| 中東 (巴林) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| 中東 (阿拉伯聯合大公國) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| 南美洲 (聖保羅) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| AWS GovCloud (美國東部) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (美國西部) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# 使用 SQL 查詢編輯器 (主控台) 查詢

介紹進階查詢的預覽功能，可讓您使用生成人工智慧 (生成 AI) 功能以純英文輸入提示，並將其轉換為 ready-to-use 查詢格式。如需詳細資訊，請參閱進階查詢的自然語言查詢處理器。

您可以使用 AWS 範例查詢，也可以建立自己稱為自訂查詢的查詢。

## 考量事項

先決條件

如果您使用下列其中一個 AWS 受管理的策略，您將擁有執行和儲存查詢的必要權限：AWSServiceRoleForConfig(服務連結角色) 或 AW ConfigRole S_。

否則，您必須擁有受AWSConfigUserAccess AWS 管理策略中包含的權限。

您可以查詢的屬性清單

中提供了更新的性質清單及其資料類型GitHub。

進階查詢和彙總器

若要在彙整工具上執行查詢，請建立彙整工具。如需詳細資訊，請參閱 使用主控台設定彙整。

如果已設定好彙整工具，請在查詢範圍中選擇彙整工具，以在該彙整工具上執行進階查詢。選取彙總器時，請考慮在查詢陳述式中新增 AWS 帳戶 ID 和 AWS Region，以便在結果中檢視該資訊。

## 使用範 AWS 例查詢

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在左側導覽中選擇 進階查詢，查詢單一帳戶和區域或是多個帳戶和區域的資源組態。
3. 在 進階查詢 頁面上，從查詢清單中選擇適當的查詢。您可以依名稱、描述、建立者或標籤來徹底篩選查詢清單。若要篩選 AWS 查詢，請選擇建立者 並輸入 AWS。您選取的查詢會顯示在 SQL 查詢編輯器中。您可以編輯選取的查詢以符合您的需求。
4. 若要將此查詢儲存至新查詢，請選擇 儲存為。
   - 請在 查詢名稱 欄位中更新查詢的名稱。
   - 請在 描述 欄位中更新查詢的描述。
   - 您可為此查詢輸入最多 50 個唯一標籤。
   - 選擇 儲存。
5. 選擇執行。查詢結果顯示於查詢編輯器下方的資料表。
6. 選擇 匯出為，以 CSV 或 JSON 格式匯出查詢結果。

> **Note**
>
> 查詢結果會以分頁顯示。選擇匯出時，最多可匯出 500 筆結果。
> 您也可以使用 API 擷取所有結果。結果會以分頁顯示，您一次可擷取 100 個結果。

## 建立自訂查詢

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在左側導覽中選擇 進階查詢，查詢單一帳戶和區域或是多個帳戶和區域的資源組態。
3. 若要建立自訂查詢，請選擇 新增查詢。

   若要檢視或編輯自訂查詢，請依名稱、描述、建立者或標籤篩選查詢。若要篩選自訂查詢，請選擇建立者 並輸入 自訂。
4. 在 查詢編輯器 頁面上，為此帳戶和區域建立您自己的查詢。您也可以選取適當的彙整工具，建立針對多個帳戶和區域的查詢。
5. 如果您希望變更此查詢，請進行編輯。若要儲存此查詢，請選擇 儲存查詢。

- 請在 查詢名稱 欄位中更新查詢的名稱。
- 請在 描述 欄位中更新查詢的描述。
- 您可為此查詢輸入最多 50 個唯一標籤。
- 選擇 儲存。

6. 選擇執行。查詢結果顯示於查詢編輯器下方的資料表。
7. 選擇 匯出為，以 CSV 或 JSON 格式匯出查詢結果。

   查詢結果會以分頁顯示。選擇匯出時，最多可匯出 500 筆結果。

   您也可以使用 API 擷取所有結果。結果會以分頁顯示，您一次可擷取 100 個結果。

# 使用 SQL 查詢編輯器 (AWS CLI) 進行查詢

AWS CLI 這是一個統一的工具來管理您的 AWS 服務。只要下載和設定一個工具，您就可以從命令列控制多個 AWS 服務，並使用指令碼將它們自動化。若要取得有關 AWS CLI 和安裝 AWS CLI 工具的更多資訊，請參閱《AWS Command Line Interface 使用指南》中的以下內容。

- AWS Command Line Interface 使用者指南
- 設定 AWS Command Line Interface

如有必要，請輸入`aws configure`以配置 AWS CLI 為使用提供進階查詢的「 AWS 區域」。

## 考量事項

先決條件

如果您使用下列其中一個 AWS 受管理的策略，您將擁有執行和儲存查詢的必要權限：AWSServiceRoleForConfig(服務連結角色) 或 AW ConfigRole S_。

否則，您必須擁有受AWSConfigUserAccess AWS 管理策略中包含的權限。

您可以查詢的屬性清單

中提供了更新的性質清單及其資料類型GitHub。

進階查詢和彙總器

若要在彙整工具上執行查詢，請建立彙整工具。如需詳細資訊，請參閱 使用主控台設定彙整。

如果已設定好彙整工具，請在查詢範圍中選擇彙整工具，以在該彙整工具上執行進階查詢。選取彙總器時，請考慮在查詢陳述式中新增 AWS 帳戶 ID 和 AWS Region，以便在結果中檢視該資訊。

## 查詢資源組態資料

若要使用查詢編輯器 (AWS CLI) 針對單一帳戶和區域查詢資源組態資料

1. 開啟命令提示或終端機視窗。
2. 輸入以下指令以查詢資源配置資料。

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

根據您的查詢，輸出如下所示：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

若要使用查詢編輯器 (AWS CLI) 針對多個帳戶和區域查詢資源組態資料

1. 開啟命令提示或終端機視窗。
2. 輸入以下指令以查詢資源配置資料。

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

根據您的查詢，輸出如下所示：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> 在進階查詢中使用`AWS::IAM::User``AWS::IAM::Group`、`AWS::IAM::Role`、和`AWS::IAM::Policy`資源類型時，請使用`awsRegion = 'global'`。

## 儲存查詢

1. 開啟命令提示或終端機視窗。
2. 輸入下列指令以儲存查詢。

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
```

```
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. 根據您的查詢，輸出如下所示：

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` 是選用的。在傳遞標籤時，`list-stored-queries` 或 `get-stored-query` 都不會傳回已儲存的標籤。您必須使用 `list-tag-for-resources` 來擷取已儲存查詢的關聯標籤。
>
> 在建立或更新查詢時，可以選擇性的使用 `--description`。

## 檢視所有儲存的查詢

1. 輸入以下指令以檢視所有已儲存查詢的清單。

```
aws configservice list-stored-queries
```

2. 根據您的查詢，輸出如下所示：

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
```

```
    ]
}
}
```

## 取得儲存查詢的詳細資訊

1. 輸入下列命令以取得特定已儲存查詢的詳細資訊。

```
aws configservice get-stored-query --query-name cli-test
```

2. 根據您的查詢，輸出如下所示：

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

## 刪除儲存的查詢

- 輸入下列指令以刪除已儲存的查詢。

```
aws configservice delete-stored-query --query-name cli-test
```

若成功的話，命令會在沒有其他輸出的情況下執行。

# 進階查詢的自然語言查詢處理器

進階查詢的自然語言查詢處理器位於的預覽版本中， AWS Config 且可能會變更。

進階查詢的自然語言查詢處理器使用 Amazon Bedrock，這是一種生成人工智慧 (生成 AI) 技術，可讓您以純英文輸入提示並將其轉換為 ready-to-use 查詢格式。使用自然語言查詢處理器，您可以查詢您的 AWS 帳戶 或整個 AWS 組織。

提示可以是問題或陳述式。例如，您可以輸入提示，例如「2024 年 1 月 1 日之後建立哪些負載平衡器？」 和「列出我正在運行節點 js 16 的所有 lambda 函數。」

## 考量事項

自然語言查詢處理器無法執行下列動作：

- 使用英文以外的語言產生查詢。
- 從與進階查詢無關的提示產生查詢。
- 從超過 1000 個字元的提示產生查詢。
- 從後續更正或先前的工作階段產生查詢。
- 解釋已生成的代碼。

## 使用自然語言查詢處理器進行查詢

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在左側導覽中選擇 進階查詢，查詢單一帳戶和區域或是多個帳戶和區域的資源組態。
3. 在進階查詢頁面上，選擇新查詢以移至 查詢編輯器。
   - (選擇性) 若要在彙總器上執行查詢，請建立彙總器。如需詳細資訊，請參閱 使用主控台設定彙整。
   - 如果已設定好彙整工具，請在查詢範圍中選擇彙整工具，並在該彙整工具上執行進階查詢。選取彙總器時，請考慮在查詢陳述式中新增 AWS 帳戶 ID 和 AWS Region，以便在結果中檢視該資訊。
4. 在查詢編輯器中，移至自然語言查詢處理器區段。以純英文輸入提示，然後選擇「產生」。如需範例，請參閱範例提示。
5. 產生查詢之後，可以選擇複製 (功能上等同於 Ctrl+C)，將查詢複製到剪貼簿，或選擇填入編輯器。如果填入編輯器，您可以編輯產生的查詢以符合您的需求。
6. 若要將此查詢儲存至新查詢，請選擇 儲存為。
   - 請在 查詢名稱 欄位中更新查詢的名稱。

- 請在 描述 欄位中更新查詢的描述。
- 您可為此查詢輸入最多 50 個唯一標籤。
- 選擇 儲存。

7. 選擇執行。查詢結果會顯示於查詢編輯器下方的資料表中。
8. 選擇 匯出為，以 CSV 或 JSON 格式匯出查詢結果。

> **Note**
>
> 查詢結果會以分頁顯示。匯出時，最多可匯出 500 筆結果。
> 您也可以使用 API 擷取所有結果。結果會以分頁顯示，您一次可擷取 100 個結果。

## 範例提示

以下是提示和生成查詢，您可以使用它們作為示例。

Example: 在 2024 年 1 月 1 日之後建立了哪些負載平衡器？

提示：What load balancers were created after January 1, 2024?

產生的查詢：

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: 我的哪些 RDS 資料庫執行個體可公開存取？

提示：Which of my RDS database instances are publicly accessible?

產生的查詢：

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: 過去一年建立了多少 EC2 執行個體？

提示：How many EC2 instances were created in last one year?

產生的查詢：

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: 我每個執行個體都有多少個 EC2 執行個體 AWS 帳戶？

提示：How many EC2 instances do I have in each of my AWS 帳戶?

產生的查詢：

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: 哪些 IAM 角色已 AdministratorAccess 附加受管政策？

提示：Which IAM roles have the managed policy AdministratorAccess attached?

產生的查詢：

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: 沒有加密的 EBS 磁碟區

提示：EBS volumes without encryption

產生的查詢：

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: 取得不合規的資源

提示：Get noncompliant resources

產生的查詢：

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: 列出我正在運行節點 js 16 的所有 lambda 函數

提示：List all my lambda function that is running node js 16

產生的查詢：

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: 哪些 ACM 憑證會在接下來的 30 天到期？

提示：What ACM certificates expire the next 30 days?

產生的查詢：

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> 產生的查詢中的時間取決於您輸入提示的時間。

## 提供回饋

您可以提供有關自然語言查詢處理器的整體意見反應，或是針對特定產生的查詢提供意見

提供有關自然語言查詢處理器的反饋

選擇右側自然語言查詢處理器上方的 [提供意見反應] 按鈕。您可以輸入您的滿意或不滿意，並提供有關如 AWS Config 何使自然語言查詢更有用的意見反應。

> **Note**
>
> 不要披露任何個人，商業敏感或機密信息。

針對特定產生的查詢提供意見反應

您可以選擇顯示在產生的查詢下方的「豎起大拇指」或「大拇指向下」按鈕，針對產生的查詢提供意見反應。

## 區域支援

下列區域支援自然語言查詢處理器。

| 區域名稱 | 區域 | 端點 | 通訊協定 |
| --- | --- | --- | --- |
| 美國東部 (維吉尼亞北部) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| 美國西部 (奧勒岡) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |

# 刪除 AWS Config 資料

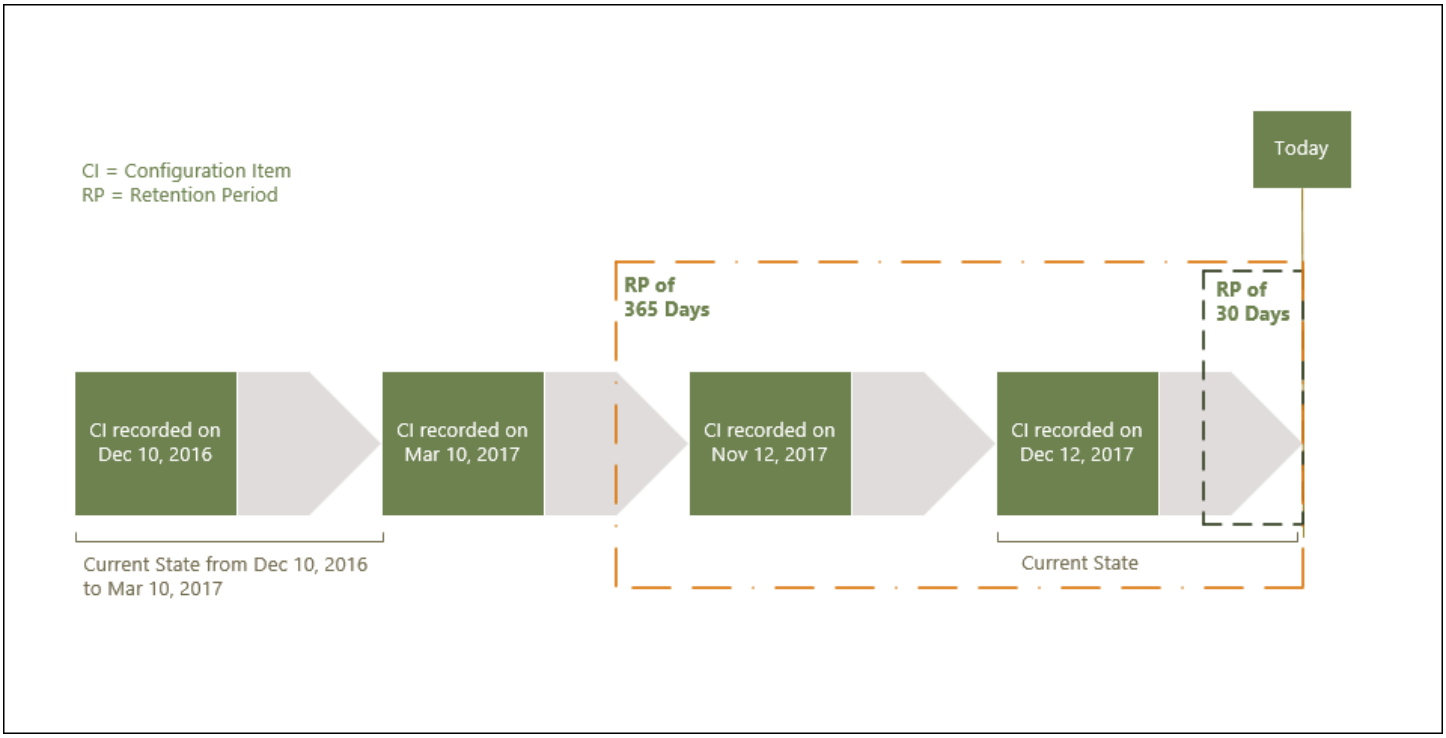
> **Note**
>
> 雖然 AWS Config 使用 Amazon Simple Storage Service (Amazon S3) 和 Amazon Simple Notification Service (Amazon SNS) 來傳送組態快照和組態歷史記錄檔案，但 AWS Config 有自己的資料存放區和保留政策。此頁面上的資訊僅適用於 AWS Config。Amazon S3 和 Amazon SNS 有各自獨立的資料存放區和保留期政策。

AWS Config 允許您通過指定的保留期限來刪除您的數據`ConfigurationItems`。當您指定保留期間時， AWS Config 會在指定的期間內保留您的`ConfigurationItems`保留期間。您可以選擇最少 30 天至最多 7 年（2557 天）之間的期限。 AWS Config 刪除超過指定保留期限的資料。若您沒有指定保留期， AWS Config 會繼續以預設期間存放 `ConfigurationItems` 達 7 年 (2557 天)。當開啟記錄時，資源目前的狀態為 `ConfigurationItem` 的記錄時間，直到記錄下一次的變更 (新的 `ConfigurationItem`)。

為了了解保留期的行為，讓我們來看看時間表。

- 當記錄開啟時，資源的目前狀態總是會存在並且無法刪除，無論 `ConfigurationItem` 記錄的日期為何。
- 新 AWS Config 記錄時`ConfigurationItems`，會根據指定`ConfigurationItems`的保留期間刪除先前的記錄。

在下列時間軸中， AWS Config 記錄`ConfigurationItems`下列日期。在此時間表中，今天為 2018 年 5 月 24 日。




下列表格說根據選取的保留期， AWS Config 時間表上顯示的 `ConfigurationItems` 為何。

| 保留期間 | 時間表上顯示的組態項目 | 說明 |
| --- | --- | --- |
| 30 天 | 2017 年 12 月 12 日 | 資源的目前狀態從 2017 年 12 月 12 日開始，即記錄 `ConfigurationItem` 的時間，並會處於有效狀態直到今天 (2018 年 5 月 24 日)。當記錄開啟時，總是會存在目前狀態。 |
| 365 天 | 2017 年 12 月 12 日；2017 年 11 月 12 日；2017 年 3 月 10 日 | 保留期會顯示目前狀態 2017 年 12 月 12 日及先前的 `ConfigurationItems` 2017 年 11 月 12 日和 2017 年 3 月 10 日。<br><br>因為 `ConfigurationItem` 代表 365 天前的目前狀態，所以 2017 年 3 月 10 日的該組態狀態會顯示在時間軸上。 |

指定保留期後， AWS Config API 就不會再傳回代`ConfigurationItems`表超過指定保留期間的狀態。

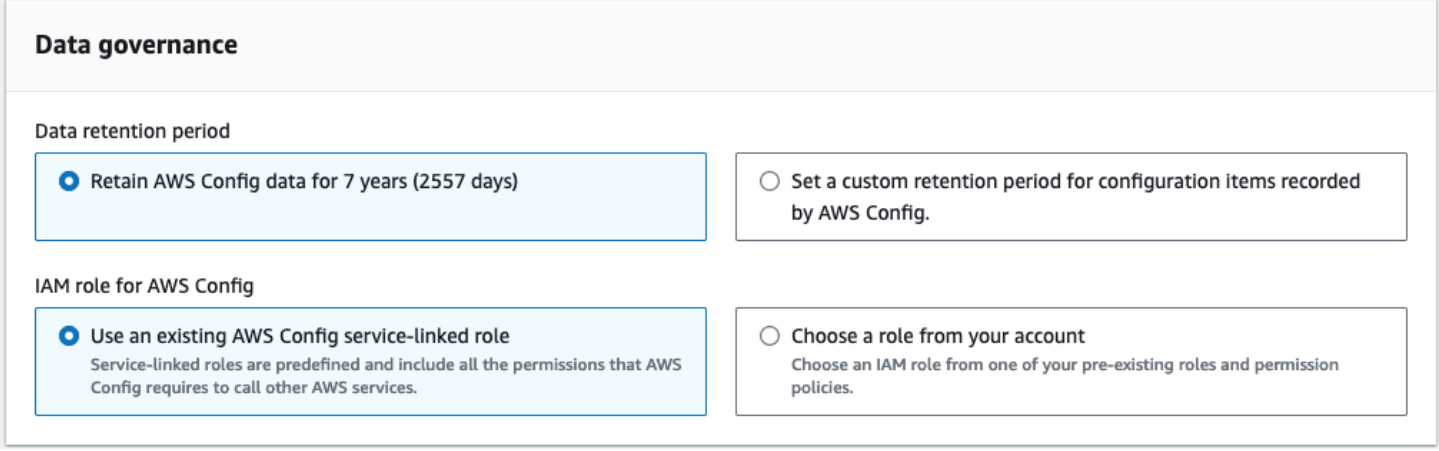
> **Note**
>
> - AWS Config `ConfigurationItems`如果錄製已關閉，則無法錄製您的。
> - AWS Config `ConfigurationItems`如果您的 IAM 角色的許可不足，則無法記錄您的。如需詳細資訊，請參閱指派給的 IAM 角色的許可 AWS Config。

## 設定資料保留期 AWS Management Console

在中 AWS Management Console，如果您未選取資料保留期間，預設期間為 7 年或 2557 天。

若要設定組態項目的自訂資料保留期，請選取核取方塊。您可以選取 1 年、3 年、5 年或自訂期間。針對自訂期間，請輸入介於 30 和 2557 天之間的天數。

下圖顯示您可以在「資料控管」中設定資料保留期間的位置。您可以從主控台存取 [編輯設定] 頁面上的 [資料 AWS Config 控管]，方法是選擇左側導覽列中的 [設定]，然後選擇 [編輯]。



# 中的安全性 AWS Config

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要瞭解適用於的規範遵循計劃 AWS Config，請參閱規範計劃AWS 服務範圍中的AWS 服務，遵的服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Config。下列主題說明如何設定 AWS Config 以符合安全性與合規性目標。

主題


- 資料保護 AWS Config
- 的 Identity and Access Management AWS Config
- 中的事件回應 AWS Config
- 符合性驗證 AWS Config
- 韌性 AWS Config
- 基礎架構安全性 AWS Config
- 預防跨服務混淆代理人
- 安全性最佳做法 AWS Config


## 資料保護 AWS Config

AWS 共同責任模型適用於 AWS Config 中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用控制台，API 或 AWS SDK AWS 服務 使用 AWS Config 或其他配置時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

## 靜態資料加密

靜態資料使用透明的伺服器端加密功能加密。這可協助降低保護敏感資料所涉及的操作負擔和複雜性。您可以透過靜態加密，建立符合加密合規和法規要求，而且對安全性要求甚高的應用程式。

## 加密傳輸中的資料

所收集和存取的資料 AWS Config 僅透過傳輸層安全性 (TLS) 受保護的通道進行存取。

# 的 Identity and Access Management AWS Config

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 AWS Config 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

主題


- 物件
- 使用身分驗證
- 使用政策管理存取權

- 如何與 IAM AWS Config 搭配使用
- 以身分識別為基礎的原則範例 AWS Config
- AWS 受管理的政策 AWS Config
- 指派給的 IAM 角色的許可 AWS Config
- 更新指派給的 IAM 角色 AWS Config
- 適用於 AWS Config 交付通道的 Amazon S3 儲存貯體的許可
- AWS Config 傳遞管道的 KMS 金鑰權限
- Amazon SNS 主題的許可
- 疑難排解 AWS Config 身分和存取
- 使用服務連結角色 AWS Config

## 物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AWS Config。

服務使用者 — 如果您使用 AWS Config 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS Config 功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS Config中的某項功能，請參閱 疑難排解 AWS Config 身分和存取。

服務管理員 — 如果您負責公司的 AWS Config 資源，您可能擁有完整的存取權 AWS Config。決定您的服務使用者應該存取哪些 AWS Config 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何搭配使用 IAM AWS Config，請參閱如何與 IAM AWS Config 搭配使用。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS Config存取權的詳細資訊。若要檢視可在 IAM 中使用的 AWS Config 基於身分的政策範例，請參閱。以身分識別為基礎的原則範例 AWS Config

## 使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料

都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

## AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

## 聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

## IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要

擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

## IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

- 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
- 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

## 使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

## 身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

## 資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

## 存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

## 其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

### 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

## 如何與 IAM AWS Config 搭配使用

在您使用 IAM 管理存取權限之前 AWS Config，請先了解哪些 IAM 功能可搭配使用 AWS Config。

您可以搭配使用的 IAM 功能 AWS Config

| IAM 功能 | AWS Config 支持 |
| --- | --- |
| 身分型政策 | 是 |
| 資源型政策 | 否 |
| 政策動作 | 是 |
| 政策資源 | 是 |
| 政策條件索引鍵 (服務特定) | 是 |
| ACL | 否 |
| ABAC (政策中的標籤) | 是 |
| 臨時憑證 | 是 |

| IAM 功能 | AWS Config 支持 |
| --- | --- |
| 轉送存取工作階段 (FAS) | 是 |
| 服務角色 | 是 |
| 服務連結角色 | 是 |

若要深入瞭解如何以 AWS Config 及其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

## 以身分識別為基礎的原則 AWS Config

| | |
| --- | --- |
| 支援身分型政策 | 是 |

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

以身分識別為基礎的原則範例 AWS Config

若要檢視以 AWS Config 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS Config

## 以資源為基礎的政策 AWS Config

| | |
| --- | --- |
| 支援以資源基礎的政策 | 否 |

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

## 的政策動作 AWS Config

| | |
|---|---|
| 支援政策動作 | 是 |

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS Config 動作清單，請參閱服務授權參考 AWS Config中所定義的動作。

中的策略動作在動作之前 AWS Config 使用下列前置詞：

```
config
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "config:Describe*"
```

若要檢視以 AWS Config 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS Config

## 的政策資源 AWS Config

| | |
|---|---|
| 支援政策資源 | 是 |

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 AWS Config 資源類型及其 ARN 的清單，請參閱服務授權參考 AWS Config中的定義資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Config定義的動作。

若要檢視以 AWS Config 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS Config

## 的政策條件索引鍵 AWS Config

| | |
|---|---|
| 支援服務特定政策條件金鑰 | 是 |

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素 (或 `Condition` 區塊) 可讓您指定使陳述式生效的條件。`Condition` 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 `Condition` 元素，或是在單一 `Condition` 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 AWS Config 條件索引鍵清單，請參閱服務授權參考 AWS Config中的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱定義的動作 AWS Config。

若要檢視以 AWS Config 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS Config

## ACL 在 AWS Config

| | |
|---|---|
| 支援 ACL | 否 |

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

## 阿巴克與 AWS Config

| | |
|---|---|
| 支援 ABAC (政策中的標籤) | 是 |

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱 IAM 使用者指南中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的使用屬性型存取控制 (ABAC)。

如需標記 AWS Config 資源的詳細資訊，請參閱 為您的 AWS Config 資源建立標籤。

## 使用臨時登入資料 AWS Config

| | |
|---|---|
| 支援臨時憑證 | 是 |

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

## 轉寄存取工作階段 AWS Config

| | |
|---|---|
| 支援轉寄存取工作階段 (FAS) | 是 |

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

## AWS Config的服務角色

| | |
|---|---|
| 支援服務角色 | 是 |

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。

> **Warning**
> 變更服務角色的權限可能會中斷 AWS Config 功能。只有在 AWS Config 提供指引時才編輯服務角色。

## 服務連結角色 AWS Config

| | |
|---|---|
| 支援服務連結角色 | 是 |

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關建立或管理 AWS Config 服務連結角色的詳細資訊，請參閱使用服務連結角色 AWS Config。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

# 以身分識別為基礎的原則範例 AWS Config

根據預設，使用者和角色不具備建立或修改 AWS Config 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需有關由所定義之動作和資源類型的詳細資訊 AWS Config，包括每個資源類型的 ARN 格式，請參閱服務授權參考 AWS Config中的動作、資源和條件索引鍵。

主題


- 政策最佳實務
- 註冊一個 AWS 帳戶
- 建立具有管理權限的使用者
- 使用 AWS Config 主控台

- 允許使用者檢視他們自己的許可
- 唯讀存取權 AWS Config
- 完全存取 AWS Config
- AWS Config 規則 API 動作支援的資源層級權限
- 支援多帳戶多區域資料彙總的資源層級許可

## 政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 AWS Config 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您的使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

## 註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

## 建立具有管理權限的使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。
2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

## 使用 AWS Config 主控台

若要存取 AWS Config 主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. AWS Config 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用 AWS Config 主控台，請同時將 AWS Config `AWSConfigUserAccess` AWS 受管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

您必須授與使用者互動的權限 AWS Config。對於需要完整存取權的使用者 AWS Config，請使用受 AWS Config管理策略的完整存取權限。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

  建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。
- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。

- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

## 允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

## 唯讀存取權 AWS Config

下列範例顯示授與唯讀存取權AWSConfigUserAccess的 AWS 受管理原則 AWS Config。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

在政策陳述式中，Effect 元素指定允許或拒絕動作。Action 元素列出允許使用者執行的特定動作。Resource 元素列出使用者得以執行特定動作的 AWS 資源。對於控制 AWS Config 動作存取權的原則，Resource元素一律會設定為*，萬用字元表示「所有資源」。

Action 元素中的值對應至服務所支援的 API。這些動作的前面會加上 config:，意指其參照 AWS Config 動作。您可以在 Action 元素中使用 * 萬用字元，如下列範例所示：

- "Action": ["config:*ConfigurationRecorder"]

這允許所有以 "ConfigurationRecorder" (`StartConfigurationRecorder`,`StopConfigurationRecorder`) 結尾的 AWS Config 動作。

- `"Action": ["config:*"]`

  這允許所有 AWS Config 操作，但不允許其他 AWS 服務的操作。

- `"Action": ["*"]`

  這允許所有 AWS 操作。此權限適用於以您帳戶 AWS 管理員身分的使用者。

唯讀政策不會將 `StartConfigurationRecorder`、`StopConfigurationRecorder` 和 `DeleteConfigurationRecorder` 動作的許可授予使用者。使用此政策的使用者無法啟動組態記錄器、停止組態記錄器．或是刪除組態記錄器。有關 AWS Config 操作列表，請參閱 AWS Config API 參考。

## 完全存取 AWS Config

下列範例顯示授與完整存取權的策略 AWS Config。它授予用戶執行所有 AWS Config 操作的權限。這也可以讓使用者管理 Amazon S3 儲存貯體中的檔案，以及管理與使用者相關聯帳戶中的 Amazon SNS 主題。

> **Important**
>
> 此政策會授予廣泛許可。授予完整存取之前，請考慮從最少的一組許可開始，然後依需要授予其他許可。這比一開始使用太寬鬆的許可，爾後再嘗試限縮許可更為安全。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
```

```
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

## AWS Config 規則 API 動作支援的資源層級權限

資源層級權限是指定允許使用者對哪些資源執行動作的能力。 AWS Config 支援特定 AWS Config 規則 API 動作的資源層級權限。這表示對於某些 AWS Config 規則動作，您可以控制允許使用者使用這些動作的條件。這些條件可以是必須滿足的動作，也可以是允許使用者使用的特定資源。

下表說明目前支援資源層級權限的 AWS Config 規則 API 動作。另說明每個動作支援的資源及其 ARN。指定 ARN 時，您可在路徑中使用 * 萬用字元，例如當您無法或不想明確指定資源 ID 時。

> **Important**
>
> 如果此表格中未列出 AWS Config 規則 API 動作，則不支援資源層級權限。如果 AWS Config 規則動作不支援資源層級權限，您可以授與使用者使用該動作的權限，但必須為政策陳述式的資源元素指定 *。

| API 動作 | 資源 |
| --- | --- |
| DeleteConfig規則 | Config 規則<br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| DeleteEvaluation結果 | Config 規則<br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| DescribeComplianceByConfig規則 | Config 規則<br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| DescribeConfigRuleEvaluation狀態 | Config 規則<br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| GetComplianceDetailsByConfigRule | Config 規則<br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| PutConfig規則 | Config 規則<br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |

| API 動作 | 資源 |
| --- | --- |
| StartConfigRulesEvaluation | Config 規則<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| PutRemediation配置 | 修補組態<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config ####/#### id* |
| DescribeRemediation配置 | 修補組態<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config ####/#### id* |
| DeleteRemediation配置 | 修補組態<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config ####/#### id* |
| PutRemediation例外 | 修補組態<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config ####/#### id* |
| DescribeRemediation例外 | 修補組態<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config ####/#### id* |
| DeleteRemediation例外 | 修補組態<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config ####/#### id* |

例如，您希望允許特定使用者的讀取存取和拒絕寫入存取特定規則。

在第一個策略中，您允許規 AWS Config 則讀取動作，例如針`DescribeConfigRuleEvaluationStatus`對指定的規則。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

在第二個策略中，您拒絕對特定 AWS Config 規則的規則寫入動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

透過資源層級權限，您可以允許讀取存取權和拒絕寫入存取權，以針對 AWS Config 規則 API 動作執行特定動作。

## 支援多帳戶多區域資料彙總的資源層級許可

您可以使用資源層級許可，控制使用者彙總多帳戶多區域資料時執行特定動作的能力。下列 AWS Config `Aggregator` API 支援資源層級權限：

- BatchGetAggregateResourceConfig
- DeleteConfiguration聚合器
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSources狀態
- GetAggregateComplianceDetailsByConfig規則
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResource計數
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfiguration聚合器
- SelectAggregateResourceConfig

例如，您可以建立兩個彙總工具 `AccessibleAggregator` 和 `InAccessibleAggregator`，然後連接允許存取 `AccessibleAggregator` 但拒絕存取 `InAccessibleAggregator` 的 IAM 政策，藉以限制特定使用者存取資源資料。

適用於的 IAM 政策 AccessibleAggregator

在此政策中，您允許存取您所指定之 AWS Config Amazon Resource Name (ARN) 支援的彙總工具動作。在此範例中， AWS Config ARN 為`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
```

```
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

適用於的 IAM 政策 InAccessibleAggregator

在此原則中，您拒絕存取所指定 AWS Config ARN 支援的彙總器動作。在此範例中， AWS Config ARN 為`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
```

```
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

如果開發人員群組的使用者嘗試在您指定的 AWS Config ARN 上執行任何這些動作，該使用者將會收到拒絕存取的例外狀況。

檢查使用者存取許可

若要顯示您已建立的彙總器，請執行下列 AWS CLI 命令：

```
aws configservice describe-configuration-aggregators
```

命令順利完成後，您將可看到與您帳戶相關聯之所有彙總工具的詳細資訊。此範例中的彙總工具為 `AccessibleAggregator` 和 `InAccessibleAggregator`：

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
```

```
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> 針對 `account-aggregation-sources`，請輸入您希望彙整資料的 AWS 帳戶 ID 逗點分隔清單。以方括弧包圍帳戶 ID，並確認逸出雙引號 (例如，`"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`)。

將以下 IAM 政策連接至 `InAccessibleAggregator` 的拒絕存取，或您想要的彙總工具拒絕存取。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
```

```
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

接著，您可以確認 IAM 政策可正常執行特定彙總工具規則的限制存取：

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

此命令應會傳回拒絕存取例外狀況：

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

## AWS 受管理的政策 AWS Config

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

## AWS 受管理的策略：AWSConfigServiceRolePolicy

AWS Config 使用指AWSServiceRoleForConfig定的服務連結角色代表您呼叫其他 AWS 服務。當您使用進行設 AWS Management Console 定時 AWS Config， AWS Config 如果您選取使用 SLR 的選項，而不是您自己的 AWS Identity and Access Management (IAM) 服務角色，則會自動建立此 AWS Config SLR。

AWSServiceRoleForConfig SLR 包含受管政策 `AWSConfigServiceRolePolicy`。此受管理的原則包含 AWS Config 資源的唯讀和唯寫權限，以及其他支援之服務中資源的 AWS Config 唯讀權限。如需詳細資訊，請參閱 支援的資源類型 及 使用服務連結角色 AWS Config。

檢視政策：AWSConfigServiceRolePolicy。

## AWS 受管理的策略：AWS_ConfigRole

若要記錄您的 AWS 資源組態， AWS Config 需要 IAM 許可以取得有關資源的組態詳細資料。如果想要為 AWS Config建立 IAM 角色，您可以使用受管政策 `AWS_ConfigRole` 並將其連接到 IAM 角色。

每次新 AWS Config 增 AWS 資源類型支援時，都會更新此 IAM 政策。這表示只要 AWS_ ConfigRole 角色已附加此受管理原則，就 AWS Config 會繼續擁有記錄支援資源類型之組態資料的必要權限。如需詳細資訊，請參閱 支援的資源類型 及 指派給的 IAM 角色的許可 AWS Config。

檢視以下原則：AWS_ ConfigRole。

## AWS 受管理的策略：AWSConfigUserAccess

此 IAM 政策提供使用權限 AWS Config，包括按資源上的標籤搜尋和讀取所有標籤。這不會提供設定權限 AWS Config，因此需要管理權限。

檢視政策：AWSConfigUserAccess。

## AWS 受管理的策略：ConfigConformsServiceRolePolicy

若要部署和管理一致性套件， AWS Config 需要 IAM 許可和其他 AWS 服務的特定許可。這些功能可讓您部署和管理具有完整功能的一致性套件，並且每次新 AWS Config 增一致性套件的新功能時都會更新。如需一致性套件的詳細資訊，請參閱《一致性套件》。

檢視原則：ConfigConformsServiceRole原則。

## AWS 受管理的策略：AWSConfigRulesExecutionRole

若要部署 AWS 自訂 Lambda 規則， AWS Config 需要 IAM 許可和來自其他 AWS 服務的特定許可。這些 AWS Lambda 功能可讓函數存取 AWS Config API 和定期交 AWS Config 付給 Amazon S3 的組態快照。評估 AWS 自訂 Lambda 規則組態變更的函數需要此存取權，每次新 AWS Config 增功能時都會更新。如需 AWS 自訂 Lambda 規則的詳細資訊，請參閱建立 AWS Config 自訂 Lambda 規則和規 AWS Config則的元件。如需組態快照的詳細資訊，請參閱《概念 | 組態快照》。如需交付組態快照的詳細資訊，請參閱《管理交付通道》。

檢視政策：AWSConfigRulesExecutionRole。

## AWS 受管理的策略：AWSConfigMultiAccountSetupPolicy

若要跨組織中的成員帳戶集中部署、更新和刪除 AWS Config 規則和一致性套件 AWS Organizations，則 AWS Config 需要 IAM 許可和其他 AWS 服務的特定許可。每次為多帳戶設定新 AWS Config 增功能時，都會更新此受管理政策。如需詳細資訊，請參閱管理組織中所有帳戶的 AWS Config 規則和管理組織中所有帳戶的一致性套件。

檢視政策：AWSConfigMultiAccountSetupPolicy。

## AWS 受管理的策略：AWSConfigRoleForOrganizations

若 AWS Config 要允許呼叫唯讀 AWS Organizations API， AWS Config 需要 IAM 許可和其他 AWS 服務的特定許可。每次為多帳戶設定新 AWS Config 增功能時，都會更新此受管理政策。如需詳細資訊，請參閱管理組織中所有帳戶的 AWS Config 規則和管理組織中所有帳戶的一致性套件。

檢視政策：AWSConfigRoleForOrganizations。

## AWS 受管理的策略：AWSConfigRemediationServiceRolePolicy

若 AWS Config 要允許代表您修復`NON_COMPLIANT`資源， AWS Config 需要 IAM 許可和其他 AWS 服務的特定許可。每次新 AWS Config 增補救功能時，此受管理策略都會更新。如需有關修正的詳細資訊，請參閱使用規則修復不符合 AWS Config 資源。如需有關啟動可能 AWS Config 評估結果之條件的詳細資訊，請參閱概念 | AWS Config 規則。

檢視政策：AWSConfigRemediationServiceRolePolicy。

## AWS ConfigAWS 受管理策略的更新

檢視 AWS Config 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 AWS Config 文件歷史記錄」頁面上的 RSS 摘要。

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource" | 此政策現在支援亞 Amazon Elastic File System (Amazon EFS)、Amazon Redshift 和 適用於 SAP 的 AWS Systems Manager. | 2024年6月17日 |
| AWSConfigServiceRolePolicy – 新增 elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource" | 此政策現在支援亞 Amazon Elastic File System (Amazon EFS)、Amazon Redshift 和 適用於 SAP 的 AWS Systems Manager. | 2024年6月17日 |
| AWS_ConfigRole – 新增 "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift- | 此政策現在支援 Prometheus、Amazon、Amazon Cognito、Amazon、Amazon FSX、 AWS Identity and Access Management (IAM) CloudWatch、、、Amazon Redshift 無伺服器 ElastiCache AWS Glue、Amazon 和亞馬遜簡單通知服務 (Amazon SNS) 的亞馬遜 SageMaker受管服務的其他許可。 AWS Lambda AWS RAM | 2024年2月22 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:GetSMSSandboxAccountStatus" | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments, | 此政策現在支援 Prometheus、Amazon、Amazon Cognito、Amazon、Amazon FSX、 AWS Identity and Access Management (IAM) CloudWatch、、、Amazon Redshift 無伺服器 ElastiCache AWS Glue、Amazon 和亞馬遜簡單通知服務 (Amazon SNS) 的亞馬遜 SageMaker受管服務的其他許可。 AWS Lambda AWS RAM | 2024年2月22 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| " and "sns:GetSMSSandboxAccountStatus" | | |
| AWSConfigUserAccess—AWS Config 開始追蹤此 AWS 受管理政策的變更 | 此原則提供使用權限 AWS Config，包括按資源上的標籤搜尋和讀取所有標籤。這不會提供設定權限 AWS Config，因此需要管理權限。 | 2024年2月22 日 |
| AWS_ConfigRole – 新增 "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets" | 此政策現在支援適用於 Prometheus AWS AppConfig、()、 AWS Database Migration Service (AWS DMSAWS Identity and Access Management) IAM 的 Amazon 受管服務、Apache 卡夫卡 (Amazon MSK)、Amazon CloudWatch 日誌和 Amazon 簡單儲存服務 (Amazon S3) 的其他許可。 AWS Organizations | 2023 年 12 月 5 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets" | 此政策現在支援適用於 Prometheus AWS AppConfig 、()、 AWS Database Migration Service (AWS DMSAWS Identity and Access Management) IAM 的 Amazon 受管服務、Apache 卡夫卡 (Amazon MSK)、Amazon CloudWatch 日誌和 Amazon 簡單儲存服務 (Amazon S3) 的其他許可。 AWS Organizations | 2023 年 12 月 5 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA | 此政策現在支援 Amazon Cognito、Amazon Connect、Amazon EMR、AWS Ground Station AWS Mainframe Modernization、Amazon MemoryDB AWS Organizations、Amazon 關係資料庫服務 (Amazon RDS)、Amazon Redshift、Amazon 路線 53 和. QuickSight AWS Service Catalog AWS Transfer Family | 2023 年 11 月 17 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations," | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles" | | |
| AWS_ConfigRole – 新增 "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID" | 此政策現在會新增`AWSConfigServiceRolePolicyStatementID` 、`AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 和 `AWSConfigSLRApiGatewayStatementID` 的安全性識別碼 (SID)。 | 2023 年 11 月 17 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA | 此政策現在支援 Amazon Cognito、Amazon Connect、Amazon EMR、AWS Ground Station AWS Mainframe Modernization、Amazon MemoryDB AWS Organizations、Amazon 關係資料庫服務 (Amazon RDS)、Amazon Redshift、Amazon 路線 53 和. QuickSight AWS Service Catalog AWS Transfer Family | 2023 年 11 月 17 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations," | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles" | | |
| AWSConfigServiceRolePolicy – 新增 "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID" | 此政策現在會新增`AWSConfigServiceRolePolicyStatementID` 、`AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 和 `AWSConfigSLRApiGatewayStatementID` 的安全性識別碼 (SID)。 | 2023 年 11 月 17 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags, | 該政策現在支持 Amazon Connect AWS Private CA AWS App Mesh，Amazon Elastic Container Service (Amazon ECS)，Amazon CloudWatch 顯然，Amazon 託管 Grafana，Amazon，亞 Amazon Inspector 器 GuardDuty，Amazon Managed Streaming for Apache Kafka（Amazon MSK） AWS IoT TwinMaker ，，，和 Amazon 的其他許可。 AWS IoT AWS Lambda AWS Network Manager AWS Organizations SageMaker | 2023 年 10 月 4 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| " "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob" | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags, | 該政策現在支持 Amazon Connect AWS Private CA AWS App Mesh，Amazon Elastic Container Service (Amazon ECS)，Amazon CloudWatch 顯然，Amazon 託管 Grafana，Amazon，亞 Amazon Inspector 器 GuardDuty，Amazon Managed Streaming for Apache Kafka（Amazon MSK） AWS IoT TwinMaker ，，，和 Amazon 的其他許可。 AWS IoT AWS Lambda AWS Network Manager AWS Organizations SageMaker | 2023 年 10 月 4 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| " "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob" | | |
| AWSConfigServiceRolePolicy— 移除 "ssm:GetParameter" | 此原則現在會移除 AWS Systems Manager (Systems Manager) 的權限。 | 2023 年 9 月 6 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets", | 此政策現在支援 Apache 卡夫卡 AWS App Mesh AWS CloudFormation、Amazon 瑪奇 CloudFront AWS CodeArtifact、 AWS CodeBuild 、、、Amazon 路線 53 AWS Glue GuardDuty、亞 Amazon Inspector 遜簡單儲存服務 AWS Identity and Access Management (Amazon S3) 和 Amazon 簡單通知服務 (Amazon SNS) 的、Amazon 管理串流 AWS Elemental MediaConnect、、 AWS Network Manager AWS Organizations、Amazon Connect AWS 資源總管、、亞馬遜連接、亞馬遜、(IAM)、亞馬遜管理串流的額外許可。AWS IoT AWS IoT TwinMaker AWS IoT Wireless | 2023 年 7 月 28 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy" | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets", "macie2:ListTagsForResource", | 此政策現在支援 Amazon AppStream 2.0 AWS App Mesh,, Amazon,, AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact, Amazon AWS CodeBuild, AWS Identity and Access Management (IAM) AWS Glue, Amazon 檢查器 GuardDuty,,, Amazon 管理流的額外許可 AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon 卡夫卡, Amazon Macie 奇,,,, Amazon 路線 53 AWS Elemental MediaConnect AWS Network Manager AWS Organizations AWS 資源總管, 亞馬遜 Simple Storage Service (Amazon S3), 亞馬遜 Simple Notification Service (Amazon SNS), 和 Amazon EC2 Systems Manager (SSM). | 2023 年 7 月 28 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource" | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa | 該政策現在支持其他許可 AWS Amplify, Amazon Connect AWS App Mesh,, Amazon 雅典娜,,, Amazon DynamoDB, Amazon DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch 明顯, Amazon Forecast,,, (IAM) AWS Organizations, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management (Amazon MSK), Amazon Lightsail, 亞 Amazon Pinpoint CloudWatch 日誌, 亞 Amazon Virtual Private Cloud AWS Elemental MediaConnect, AWS Elemental MediaTailor 亞馬遜 AWS IoT Greengrass AWS Ground Station VPC），Amazon Personalize 化，Amazon QuickSight AWS Migration Hub Refactor Spaces，Amazon Simple Storage Service (Amazon S3)，Amazon SageMaker，AWS Transfer Family。 | 2023 年 6 月 13 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "org | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| anizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource" | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast | 該政策現在支持其他許可 AWS Amplify, Amazon Connect AWS App Mesh,, Amazon 雅典娜,,, Amazon DynamoDB, Amazon DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch 明顯, Amazon Forecast,,, (IAM) AWS Organizations, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management (Amazon MSK), Amazon Lightsail, 亞 Amazon Pinpoint CloudWatch 日誌, 亞 Amazon Virtual Private Cloud AWS Elemental MediaConnect, AWS Elemental MediaTailor 亞馬遜 AWS IoT Greengrass AWS Ground Station VPC），Amazon Personalize 化，Amazon QuickSight AWS Migration Hub Refactor Spaces，Amazon Simple Storage Service (Amazon S3)，Amazon SageMaker，AWS Transfer Family。 | 2023 年 6 月 13 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAcc | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource" | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat | 此政策現在支援 Amazon 受管工作流程的 AWS Amplify 額外許可 CloudFront,, AWS CodeArtifact, Amazon 彈性運算雲, Amazon 肯德拉, Amazon Macie, Amazon 路線 53, Amazon SageMaker, Amazon Pinpoint AWS Transfer Family, AWS 彈性中樞 AWS Migration Hub, Amazon, AWS Directory Service CloudWatch, 和. AWS App Mesh AWS App Runner AWS WAF | 2023 年 4 月 13 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ion，macie2:GetClassificationExportConfiguration，macie2:GetCustomDataIdentifier，macie2:GetFindingsPublicationConfiguration，macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel，refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments，resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition，sagemaker:DescribeModelQualityJobDefinition，sagemaker:DescribePipeline, sagemaker:DescribeProject，sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions，sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines，sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificati | 此政策現在支援 Amazon 受管工作流程的 AWS Amplify 額外許可 CloudFront,, AWS CodeArtifact, Amazon 彈性運算雲, Amazon 肯德拉, Amazon Macie, Amazon 路線 53, Amazon SageMaker, Amazon Pinpoint AWS Transfer Family, AWS 彈性中樞 AWS Migration Hub, Amazon, AWS Directory Service CloudWatch, 和. AWS App Mesh AWS App Runner AWS WAF | 2023 年 4 月 13 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| onExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resilienchub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 appflow:DescribeFlow，appflow:ListFlows，appflow:ListTagsForResource，apprunner:DescribeService，apprunner:ListServices，apprunner:ListTagsForResource，appstream:DescribeApplications，appstream:DescribeFleets，cloudfront:GetResponseHeadersPolicy，cloudwatch:ListTagsForResource，codeartifact:DescribeRepository，codeartifact:GetRepositoryPermissionsPolicy，codeartifact:ListTagsForResource，codecommit:GetRepository，codecommit:GetRepositoryTriggers， codecommit:ListRepositories，codecommit:ListTagsForResource，devicefarm:GetInstanceProfile，devicefarm:ListInstanceProfiles，devicefarm:ListProjects，evidently:GetProject，evidently:ListProjects，evidently:ListTagsForResource，forecast:DescribeDataset，forecast:ListDatasets，forecast:ListTagsForResource，groundstation:GetConfig，groundstation:ListConfigs，groundstation:ListTagsForResource，iam:GetInstanceProfile，iam:GetSAML | 此政策現在支援 Amazon 管理工作流程的其他許可 AppFlow AWS App Runner CloudFront，Amazon AppStream 2.0 CloudWatch，Amazon AWS CodeArtifact， AWS CodeCommit Amazon AWS Device Farm，Amazon CloudWatch 預測， AWS Identity and Access Management（IAM）， AWS Ground Station Amazon MemoryDB AWS IoT，Amazon 針點，亞馬 Amazon Relational Database Service（Amazon RDS），Amazon Redshift 和 Amazon。 AWS Network Manager AWS Panorama SageMaker | 2023 年 3 月 30 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| Provider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundsta | 此政策現在支援 Amazon、Amazon AppStream 2.0 AppFlow、Amazon AWS App Runner、Amazon 彈性運算雲 (Amazon EC2) CloudWatch AWS CodeArtifact AWS CodeCommit AWS Device Farm、Amazon CloudWatch Elastic Compute Cloud (Amazon EC2)、Amazon 預測、 AWS Identity and Access Management (IAM) AWS Ground Station AWS IoT、Amazon MemoryDB 的額外許可，Amazon Pinpoint 關係資料庫服務 (Amazon RDS)、Amazon Redshift 和 Amazon。 AWS CloudFormation CloudFront AWS Network Manager AWS Panorama SageMaker | 2023 年 3 月 30 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| tion:GetConfig，groundstation:ListConfigs，groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate，iam:ListAccessKeys，iam:ListGroups，iam:ListInstanceProfiles，iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles，iam:ListSAMLProviders，iot:DescribeFleetMetric，iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags，mobiletargeting:GetApp，mobiletargeting:GetCampaigns，networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites，panorama:ListNodes，rds:DescribeDBProxyEndpoints，redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig，sagemaker:DescribeImage，sagemaker:DescribeImageVersion，sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigRulesExecutionRole— AWS Config 開始追蹤此 AWS 受管理政策的變更 | 此政策允許 AWS Lambda 函數存取 AWS Config API 和定期交 AWS Config 付給 Amazon S3 的組態快照。評估 AWS 自訂 Lambda 規則之組態變更的函數需要此存取權。 | 2023 年 3 月 7 日 |
| AWSConfigRoleForOrganizations— AWS Config 開始追蹤此 AWS 受管理政策的變更 | 此原則允 AWS Config 許呼叫唯讀 AWS Organizations API。 | 2023 年 3 月 7 日 |
| AWSConfigRemediationServiceRolePolicy— AWS Config 開始追蹤此 AWS 受管理政策的變更 | 此原則允 AWS Config 許代表您修復`NON_COMPLIANT` 資源。 | 2023 年 3 月 7 日 |
| AWSConfigServiceRolePolicy – 新增 auditmanager:GetAccountStatus | 此政策現在會授予可傳回 AWS Audit Manager帳戶註冊狀態的許可。 | 2023 年 3 月 3 日 |
| AWS_ConfigRole – 新增 auditmanager:GetAccountStatus | 此政策現在會授予可傳回 AWS Audit Manager帳戶註冊狀態的許可。 | 2023 年 3 月 3 日 |
| AWSConfigMultiAccountSetupPolicy— AWS Config 開始追蹤此 AWS 受管理政策的變更 | 此原則 AWS Config 允許在組織中呼叫 AWS 服務和部署 AWS Config 資源 AWS Organizations。 | 2023 年 2 月 27 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 airflow:ListTagsForResource，iot:ListCustomMetrics，iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs，appstream:ListTagsForResource， codeguru-reviewer:DescribeRepositoryAssociation，codeguru-reviewer:ListRepositoryAssociations，healthlake:ListFHIRDatastores，healthlake:DescribeFHIRDatastore，healthlake:ListTagsForResource, kinesisvideo:DescribeStream，kinesisvideo:ListStreams， kinesisvideo:ListTagsForStream，kinesisvideo:DescribeSignalingChannel，kinesisvideo:ListTagsForResource，kinesisvideo:ListSignalingChannels，route53-recovery-control-config:DescribeCluster，route53-recovery-control-config:DescribeRoutingControl， route53-recovery-control-config:DescribeSafetyRule， route53-recovery-control-config:ListClusters，route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules，devicefarm:GetTestGridProject，devicefarm:L | 此政策現在支援 Apache 氣流、Amazon AppStream 2.0、Amazon CodeGuru 審閱者 AWS IoT、Amazon Kinesis 影片串流、Amazon 路線 53 應用程式恢復控制器、Amazon 彈性運算雲端 (Amazon EC2) AWS Device Farm、Amazon 針點 AWS Identity and Access Management (IAM)、亞馬遜和亞馬遜日誌的其他管理工作流程的許可。 AWS HealthLake GuardDuty CloudWatch | 2023 年 2 月 1 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| istTestGridProjects，ec2:DescribeCapacityReservationFleets，ec2:DescribeIpamPools， ec2:DescribeIpams，ec2:GetInstanceTypesFromInstanceRequirement，mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource，ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination，logs:GetLogDelivery, and logs:ListLogDeliveries | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar | 此政策現在支援 Apache 氣流、Amazon AppStream 2.0、Amazon CodeGuru 審閱者 AWS IoT、Amazon Kinesis 影片串流、Amazon 路線 53 應用程式恢復控制器、Amazon 彈性運算雲端 (Amazon EC2) AWS Device Farm、Amazon 針點 AWS Identity and Access Management (IAM)、亞馬遜和亞馬遜日誌的其他管理工作流程的許可。 AWS HealthLake GuardDuty CloudWatch | 2023 年 2 月 1 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries | | |
| ConfigConformsServiceRolePolicy – 更新 config:DescribeConfigRules | 作為安全最佳實務，此政策現可移除 `config:DescribeConfigRules` 的廣泛資源層級許可。 | 2023 年 1 月 12 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor | 此政策現在支援針對 Prometheus、、、、()、 AWS Audit Manager Amazon 彈性運算雲端 AWS Database Migration Service (Amazon EC2 AWS DMS)、 AWS Directory Service、、Amazon Lightsail、、Amazon AWS Glue、 AWS IoT亞馬遜路線 53 應用程式復原控制器 AWS Elemental MediaPackage AWS Network Manager QuickSight AWS Resource Access Manager、亞馬遜簡單儲存服務 (Amazon S3) 和 Amazon Timestream 的亞馬遜受管服務的額外許可。 AWS Device Farm | 2022 年 12 月 15 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| Resource，quicksight:DescribeDashboard，quicksight:DescribeDashboardPermissions，quicksight:DescribeTemplate，quicksight:DescribeTemplatePermissions， quicksight:ListDashboards， quicksight:ListTemplates， ram:ListResources，route53-recovery-control-config:DescribeControlPanel，route53-recovery-control-config:ListControlPanels，route53-recovery-control-config:ListTagsForResource，route53resolver:GetResolverQueryLogConfigAssociation，route53resolver:ListResolverQueryLogConfigAssociations， s3:GetAccessPointForObjectLambda，s3:GetAccessPointPolicyForObjectLambda，s3:GetAccessPointPolicyStatusForObjectLambda，s3:GetMultiRegionAccessPoint，s3:ListAccessPointsForObjectLambda，s3:ListMultiRegionAccessPoints， timestream:DescribeEndpoints，transfer:DescribeConnector，transfer:ListConnectors， and transfer:ListTagsForResource | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 APS:DescribeRuleGroupsNamespace，APS:DescribeWorkspace，APS:ListWorkspaces，auditmanager:GetAssessment， auditmanager:ListAssessments，devicefarm:GetNetworkProfile，devicefarm:GetProject，devicefarm:ListNetworkProfiles，devicefarm:ListTagsForResource，dms:DescribeEndpoints，ds:ListTagsForResource，ec2:DescribeTags，ec2:DescribeTrafficMirrorSessions，ec2:DescribeTrafficMirrorTargets，ec2:GetIpamPoolAllocations， ec2:GetIpamPoolCidrs， glue:GetMLTransform， glue:GetMLTransforms，glue:ListMLTransforms，iot:DescribeScheduledAudit，iot:ListScheduledAudits，ivs:GetChannel，lightsail:GetRelationalDatabases，mediapackage-vod:DescribePackagingConfiguration，mediapackage-vod:ListPackagingConfigurations，networkmanager:DescribeGlobalNetworks， networkmanager:GetTransitGatewayRegistrations， networkmanager:ListTagsFor | 此政策現在支援針對 Prometheus、、、、()、 AWS Audit Manager Amazon 彈性運算雲端 AWS Database Migration Service (Amazon EC2 AWS DMS)、 AWS Directory Service、、Amazon Lightsail、、Amazon AWS Glue、 AWS IoT亞馬遜路線 53 應用程式復原控制器 AWS Elemental MediaPackage AWS Network Manager QuickSight AWS Resource Access Manager、亞馬遜簡單儲存服務 (Amazon S3) 和 Amazon Timestream 的亞馬遜受管服務的額外許可。 AWS Device Farm | 2022 年 12 月 15 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| Resource，quicksight:DescribeDashboard，quicksight:DescribeDashboardPermissions，quicksight:DescribeTemplate，quicksight:DescribeTemplatePermissions， quicksight:ListDashboards， quicksight:ListTemplates， ram:ListResources，route53-recovery-control-config:DescribeControlPanel，route53-recovery-control-config:ListControlPanels，route53-recovery-control-config:ListTagsForResource，route53resolver:GetResolverQueryLogConfigAssociation，route53resolver:ListResolverQueryLogConfigAssociations， s3:GetAccessPointForObjectLambda，s3:GetAccessPointPolicyForObjectLambda，s3:GetAccessPointPolicyStatusForObjectLambda，s3:GetMultiRegionAccessPoint，s3:ListAccessPointsForObjectLambda，s3:ListMultiRegionAccessPoints， timestream:DescribeEndpoints，transfer:DescribeConnector，transfer:ListConnectors， and transfer:ListTagsForResource | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 cloudformation:ListStackResources and cloudformation:ListStacks | 此原則現在會授與傳回指定堆疊之所有資源描述的權限，並傳回狀態符合指定之 AWS CloudFormation 堆疊之摘要資訊的權限StackStatusFilter。 | 2022 年 11 月 7 日 |
| AWS_ConfigRole – 新增 cloudformation:ListStackResources and cloudformation:ListStacks | 此原則現在會授與傳回指定堆疊之所有資源描述的權限，並傳回狀態符合指定之 AWS CloudFormation 堆疊之摘要資訊的權限StackStatusFilter。 | 2022 年 11 月 7 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersi | 該政策現在支持其他許可 AWS Certificate Manager, Amazon 管理工作流程 Apache 氣流 AWS Amplify AWS AppConfig ,, Amazon Keyspaces , Amazon CloudWatch, Amazon 雲 AWS Glue DataBrew, Amazon 彈性 Kubernetes 服務 (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon EventBridge, Amazon Location Service AWS Fault Injection Service, Amazon 萊克斯, 亞馬遜 Lightsail GameLift, 亞 Amazon Pinpoint AWS IoT, 亞馬遜 FSx, 亞馬遜 RDS 關係, 服務 (亞馬遜 QuickSight RDS AWS OpsWorks AWS Panorama AWS Resource Access Manager, 關係)Amazon Rekognition,, AWS RoboMaker, Amazon 路線 53 AWS Resource Groups, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map和. AWS Security Token Service | 2022 年 10 月 19 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ons, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsite | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| wise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| , panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersions, databrew:ListRulesets, | 該政策現在支持其他許可 AWS Certificate Manager, Amazon 管理工作流程 Apache 氣流 AWS Amplify AWS AppConfig ,, Amazon Keyspaces , Amazon CloudWatch, Amazon 雲 AWS Glue DataBrew, Amazon 彈性 Kubernetes 服務 (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon EventBridge, Amazon Location Service AWS Fault Injection Service, Amazon 萊克斯, 亞馬遜 Lightsail GameLift, 亞 Amazon Pinpoint AWS IoT, 亞馬遜 FSx, 亞馬遜 RDS 關係, 服務 (亞馬遜 QuickSight RDS AWS OpsWorks AWS Panorama AWS Resource Access Manager, 關係)Amazon Rekognition,, AWS RoboMaker, Amazon 路線 53 AWS Resource Groups, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map和. AWS Security Token Service | 2022 年 10 月 19 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsit | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage, panorama:Describe | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| PackageVersion，panorama:ListApplicationInstances，panorama:ListPackages，quicksight:ListDataSources，ram:ListResourceSharePermissions，rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors，resource-groups:GetGroup，resource-groups:GetGroupConfiguration，resource-groups:GetGroupQuery, resource-groups:GetTags，resource-groups:ListGroupResources，resource-groups:ListGroups，robomaker:ListRobotApplications，robomaker:ListSimulationApplications，route53resolver:GetResolverDnssecConfig，route53resolver:ListResolverDnssecConfigs，s3:ListStorageLensConfigurations, schemas:GetResourcePolicy，servicediscovery:ListInstances，sts:GetCallerIdentity，synthetics:GetGroup, synthetics:ListAssociatedGroups，synthetics:ListGroupResources, and synthetics:ListGroups | | |
| AWSConfigServiceRolePolicy – 新增 Glue::GetTable | 此原則現在會授與擷取指定資料 AWS Glue 表之資料目錄中之資料表定義的權限。 | 2022 年 9 月 14 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 Glue::GetTable | 此原則現在會授與擷取指定資料 AWS Glue 表之資料目錄中之資料表定義的權限。 | 2022 年 9 月 14 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirr | 該政策現在支持 Amazon，Amazon AppFlow，Amazon CloudWatch 朗姆酒 CloudWatch，Amazon CloudWatch Synthetics 料，Amazon Connect 語音 ID，Amazon DevOps 大師，Amazon Elastic Compute Cloud (Amazon EC2)，Amazon EC2 Auto Scaling，Amazon EMR，Amazon EventBridge 模式，Amazon Fraud Detector EventBridge，Amazon Amazon FinSpace，Amazon 交互式視頻服務（Amazon IVS）GameLift，亞馬遜 Flink，EC2 Image Builder，亞馬遜 Lightsail，亞馬遜 Lex 的亞馬遜託管服務Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon 敏捷 StudioAmazon Pinpoint QuickSight, Amazon, Amazon 路線 53 應用程序恢復控制器,, Amazon 簡單存儲服務 (Amazon S3), Amazon Timestream,,,,,,,,,,,, AWS AppConfig,, AWS AppSync, AWS Auto Scaling, AWS Backup,, AWS Budgets, AWS Cost Explorer, AWS | 2022 年 9 月 7 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| orFilters，ec2:DescribeTrafficMirrorTargets，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint，events:DescribeEventBus，events:DescribeRule，events:ListArchives， events:ListEndpoints， events:ListEventBuses，events:ListRules，events:ListTagsForResource，events:ListTargetsByRule，finspace:GetEnvironment，finspace:ListEnvironments，frauddetector:GetDetectors，frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes，frauddetector:GetEventTypes，frauddetector:GetExternalModels，frauddetector:GetLabels, frauddetector:GetModels，frauddetector:GetOutcomes，frauddetector:GetVariables，frauddetector:ListTagsForResource，gamelift:DescribeAlias，gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity，game | Cloud9,, AWS Directory Service, AWS DataSync, Amazon Route 53 Resolver AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker、 AWS Lake Formation、 AWS License Manager AWS Resilience Hub、 AWS Signer、和 AWS Transfer Family。 | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| lift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:Desc | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, ioteventsDescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| , iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:Ge | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| tInstance，lightsail:GetInstances，lightsail:GetKeyPair，lightsail:GetLoadBalancer，lightsail:GetLoadBalancers，lightsail:GetLoadBalancerTlsCertificates，lightsail:GetStaticIp，lightsail:GetStaticIps，lookoutequipment:DescribeInferenceScheduler，lookoutequipment:ListTagsForResource，lookoutmetrics:DescribeAlert，lookoutmetrics:DescribeAnomalyDetector，lookoutmetrics:ListAlerts，lookoutmetrics:ListAnomalyDetectors，lookoutmetrics:ListMetricSets，lookoutmetrics:ListTagsForResource，lookoutvision:DescribeProject，lookoutvision:ListProjects，managedblockchain:GetMember，managedblockchain:GetNetwork，managedblockchain:GetNode，managedblockchain:ListInvitations，managedblockchain:ListMembers，managedblockchain:ListNodes，mediapackage-vod:DescribePackagingGroup，mediapackage-vod:ListPackagingGroups，mediapackage-vod:ListTagsForResource，mobiletargeting:GetInAppTemplate，mobiletargeting: | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPo | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| intPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUs | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| er, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets, | 該政策現在支持 Amazon，Amazon AppFlow，Amazon CloudWatch 朗姆酒 CloudWatch，Amazon CloudWatch Synthetics 料，Amazon Connect 語音 ID，Amazon DevOps 大師，Amazon Elastic Compute Cloud (Amazon EC2)，Amazon EC2 Auto Scaling，Amazon EMR，Amazon EventBridge 模式，Amazon Fraud Detector EventBridge，Amazon Amazon FinSpace，Amazon 交互式視頻服務（Amazon IVS）GameLift，亞馬遜 Flink，EC2 Image Builder，亞馬遜 Lightsail，亞馬遜 Lex 的亞馬遜託管服務Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon 敏捷 StudioAmazon Pinpoint QuickSight, Amazon, Amazon 路線 53 應用程序恢復控制器,, Amazon 簡單存儲服務 (Amazon S3), Amazon Timestream,,,,,,,, ,,,, AWS AppConfig,, AWS AppSync, AWS Auto Scaling, AWS Backup,, AWS Budgets, AWS Cost Explorer, AWS | 2022 年 9 月 7 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttributes, gamel | Cloud9,, AWS Directory Service, AWS DataSync, Amazon Route 53 Resolver AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker、 AWS Lake Formation AWS License Manager、 AWS Resilience Hub、 AWS Signer、和 AWS Transfer Family | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| , iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwi | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| nmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lights | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetRead | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| inessCheck，route53-recovery-readiness:GetRecoveryGroup，route53-recovery-readiness:GetResourceSet，route53-recovery-readiness:ListCells，route53-recovery-readiness:ListReadinessChecks，route53-recovery-readiness:ListRecoveryGroups，route53-recovery-readiness:ListResourceSets，route53resolver:GetFirewallDomainList，route53resolver:GetFirewallRuleGroup，route53resolver:GetFirewallRuleGroupAssociation，route53resolver:GetResolverQueryLogConfig，route53resolver:ListFirewallDomainLists，route53resolver:ListFirewallDomains，route53resolver:ListFirewallRuleGroupAssociations，route53resolver:ListFirewallRuleGroups，route53resolver:ListFirewallRules，route53resolver:ListResolverQueryLogConfigs，rum:GetAppMonitor，rum:GetAppMonitorData，rum:ListAppMonitors，rum:ListTagsForResource，s3-outposts:GetAccessPoint，s3-outposts:GetAccessPointPolicy，s3-outposts:GetBucket，s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging，s3-outposts:GetL | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer: | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, | 此政策現在支援 Apache 氣流、Amazon AppStream 2.0、Amazon CodeGuru 審閱者 AWS IoT、Amazon Kinesis 影片串流、Amazon 路線 53 應用程式恢復控制器、Amazon 彈性運算雲端 (Amazon EC2) AWS Device Farm、Amazon 針點 AWS Identity and Access Management (IAM)、亞馬遜和亞馬遜日誌的其他管理工作流程的許可。 AWS HealthLake GuardDuty CloudWatch | 2023 年 2 月 1 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar | 此政策現在支援 Apache 氣流、Amazon AppStream 2.0、Amazon CodeGuru 審閱者 AWS IoT、Amazon Kinesis 影片串流、Amazon 路線 53 應用程式恢復控制器、Amazon 彈性運算雲端 (Amazon EC2) AWS Device Farm、Amazon 針點 AWS Identity and Access Management (IAM)、亞馬遜和亞馬遜日誌的其他管理工作流程的許可。 AWS HealthLake GuardDuty CloudWatch | 2023 年 2 月 1 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| m:ListTestGridProjects，ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools，ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement，mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource，ecr:BatchGetRepositoryScanningConfiguration，iam:ListServerCertificates，guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination, logs:GetLogDelivery，and logs:ListLogDeliveries | | |
| ConfigConformsServiceRolePolicy – 更新 config:DescribeConfigRules | 作為安全最佳實務，此政策現可移除 `config:DescribeConfigRules` 的廣泛資源層級許可。 | 2023 年 1 月 12 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat | 此政策現在支援針對 Prometheus、、、、()、 AWS Audit Manager Amazon 彈性運算雲端 AWS Database Migration Service (Amazon EC2 AWS DMS)、 AWS Directory Service、、Amazon Lightsail、、Amazon AWS Glue、 AWS IoT亞馬遜路線 53 應用程式復原控制器 AWS Elemental MediaPackage AWS Network Manager QuickSight AWS Resource Access Manager、亞馬遜簡單儲存服務 (Amazon S3) 和 Amazon Timestream 的亞馬遜受管服務的額外許可。 AWS Device Farm | 2022 年 12 月 15 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ions，networkmanager:ListTagsForResource，quicksight:DescribeDashboard，quicksight:DescribeDashboardPermissions，quicksight:DescribeTemplate，quicksight:DescribeTemplatePermissions，quicksight:ListDashboards, quicksight:ListTemplates，ram:ListResources，route53-recovery-control-config:DescribeControlPanel，route53-recovery-control-config:ListControlPanels，route53-recovery-control-config:ListTagsForResource，route53resolver:GetResolverQueryLogConfigAssociation，route53resolver:ListResolverQueryLogConfigAssociations，s3:GetAccessPointForObjectLambda，s3:GetAccessPointPolicyForObjectLambda，s3:GetAccessPointPolicyStatusForObjectLambda，s3:GetMultiRegionAccessPoint，s3:ListAccessPointsForObjectLambda，s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints，transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa | 此政策現在支援針對 Prometheus、、、、()、 AWS Audit Manager Amazon 彈性運算雲端 AWS Database Migration Service (Amazon EC2 AWS DMS)、 AWS Directory Service、、Amazon Lightsail、、Amazon AWS Glue、 AWS IoT亞馬遜路線 53 應用程式復原控制器 AWS Elemental MediaPackage AWS Network Manager QuickSight AWS Resource Access Manager、亞馬遜簡單儲存服務 (Amazon S3) 和 Amazon Timestream 的亞馬遜受管服務的額外許可。 AWS Device Farm | 2022 年 12 月 15 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 cloudformation:ListStackResources and cloudformation:ListStacks | 此原則現在會授與傳回指定堆疊之所有資源描述的權限，並傳回狀態符合指定之 AWS CloudFormation 堆疊之摘要資訊的權限StackStatusFilter。 | 2022 年 11 月 7 日 |
| AWS_ConfigRole – 新增 cloudformation:ListStackResources and cloudformation:ListStacks | 此原則現在會授與傳回指定堆疊之所有資源描述的權限，並傳回狀態符合指定之 AWS CloudFormation 堆疊之摘要資訊的權限StackStatusFilter。 | 2022 年 11 月 7 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers | 該政策現在支持其他許可 AWS Certificate Manager, Amazon 管理工作流程 Apache 氣流 AWS Amplify AWS AppConfig ,, Amazon Keyspaces , Amazon CloudWatch, Amazon 雲 AWS Glue DataBrew, Amazon 彈性 Kubernetes 服務 (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon EventBridge, Amazon Location Service AWS Fault Injection Service, Amazon 萊克斯, 亞馬遜 Lightsail GameLift, 亞 Amazon Pinpoint AWS IoT, 亞馬遜 FSx, 亞馬遜 RDS 關係, 服務 (亞馬遜 QuickSight RDS AWS OpsWorks AWS Panorama AWS Resource Access Manager, 關係)Amazon Rekognition,, AWS RoboMaker, Amazon 路線 53 AWS Resource Groups, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map和. AWS Security Token Service | 2022 年 10 月 19 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers | 該政策現在支持其他許可 AWS Certificate Manager, Amazon 管理工作流程 Apache 氣流 AWS Amplify AWS AppConfig ,, Amazon Keyspaces , Amazon CloudWatch, Amazon 雲 AWS Glue DataBrew, Amazon 彈性 Kubernetes 服務 (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon EventBridge, Amazon Location Service AWS Fault Injection Service, Amazon 萊克斯, 亞馬遜 Lightsail GameLift, 亞 Amazon Pinpoint AWS IoT, 亞馬遜 FSx, 亞馬遜 RDS 關係, 服務 (亞馬遜 QuickSight RDS AWS OpsWorks AWS Panorama AWS Resource Access Manager, 關係)Amazon Rekognition,, AWS RoboMaker, Amazon 路線 53 AWS Resource Groups, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map和. AWS Security Token Service | 2022 年 10 月 19 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 Glue::GetTable | 此原則現在會授與擷取指定資料 AWS Glue 表之資料目錄中之資料表定義的權限。 | 2022 年 9 月 14 日 |
| AWS_ConfigRole – 新增 Glue::GetTable | 此原則現在會授與擷取指定資料 AWS Glue 表之資料目錄中之資料表定義的權限。 | 2022 年 9 月 14 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte | 該政策現在支持 Amazon，Amazon AppFlow，Amazon CloudWatch 朗姆酒 CloudWatch，Amazon CloudWatch Synthetics 料，Amazon Connect 語音 ID，Amazon DevOps 大師，Amazon Elastic Compute Cloud (Amazon EC2)，Amazon EC2 Auto Scaling，Amazon EMR，Amazon EventBridge 模式，Amazon Fraud Detector EventBridge，Amazon Amazon FinSpace，Amazon 交互式視頻服務（Amazon IVS） GameLift，亞馬遜 Flink，EC2 Image Builder，亞馬遜 Lightsail，亞馬遜 Lex 的亞馬遜託管服務Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon 敏捷 StudioAmazon Pinpoint QuickSight, Amazon, Amazon 路線 53 應用程序恢復控制器,, Amazon 簡單存儲服務 (Amazon S3), Amazon Timestream,,,,,,,,,,,,, AWS AppConfig, AWS AppSync,, AWS Auto Scaling, AWS Backup, AWS Budgets,, AWS | 2022 年 9 月 7 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| rs，ec2:DescribeTrafficMirrorTargets，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule, events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity, | Cost Explorer, AWS Cloud9, AWS Directory Service,, AWS DataSync, AWS Elemental MediaPackage, Amazon Route 53 Resolver AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation、 AWS License Manager AWS Resilience Hub、 AWS Signer、和 AWS Transfer Family。 | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting: | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge | 該政策現在支持 Amazon，Amazon AppFlow，Amazon CloudWatch 朗姆酒 CloudWatch，Amazon CloudWatch Synthetics 料，Amazon Connect 語音 ID，Amazon DevOps 大師，Amazon Elastic Compute Cloud (Amazon EC2)，Amazon EC2 Auto Scaling，Amazon EMR，Amazon EventBridge 模式，Amazon Fraud Detector EventBridge，Amazon Amazon FinSpace，Amazon 交互式視頻服務（Amazon IVS） GameLift，亞馬遜 Flink，EC2 Image Builder，亞馬遜 Lightsail，亞馬遜 Lex 的亞馬遜託管服務Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon 敏捷 StudioAmazon Pinpoint QuickSight, Amazon, Amazon 路線 53 應用程序恢復控制器,, Amazon 簡單存儲服務 (Amazon S3), Amazon Timestream,,,,,,,,,,,,, AWS AppConfig, AWS AppSync,, AWS Auto Scaling, AWS Backup, AWS Budgets,, AWS | 2022 年 9 月 7 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ts，ec2:GetNetworkInsightsAccessScopeAnalysisFindings， ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio， elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule, events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule， finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat | Cost Explorer, AWS Cloud9, AWS Directory Service,, AWS DataSync, AWS Elemental MediaPackage, Amazon Route 53 Resolver AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation、 AWS License Manager AWS Resilience Hub、 AWS Signer、和 AWS Transfer Family | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates, | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| olicies，route53-recovery-readiness:GetCell，route53-recovery-readiness:GetReadinessCheck，route53-recovery-readiness:GetRecoveryGroup，route53-recovery-readiness:GetResourceSet，route53-recovery-readiness:ListCells，route53-recovery-readiness:ListReadinessChecks，route53-recovery-readiness:ListRecoveryGroups，route53-recovery-readiness:ListResourceSets，route53resolver:GetFirewallDomainList，route53resolver:GetFirewallRuleGroup，route53resolver:GetFirewallRuleGroupAssociation，route53resolver:GetResolverQueryLogConfig，route53resolver:ListFirewallDomainLists，route53resolver:ListFirewallDomains，route53resolver:ListFirewallRuleGroupAssociations，route53resolver:ListFirewallRuleGroups，route53resolver:ListFirewallRules，route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor，rum:GetAppMonitorData，rum:ListAppMonitors，rum:ListTagsForResource, s3-outposts:GetAccessPoint，s3-outposts:GetAccessPoint | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource | | |
| AWSConfigServiceRolePolicy – 新增 datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists | 此政策現在授予傳回 AWS DataSync 代理程式清單、DataSync 來源和目的地位置以及 DataSync 任務的權限 AWS 帳戶；列出與中一個或多個指定 AWS Cloud Map 命名空間關聯的命名空間和服務的摘要資訊 AWS 帳戶；並列出中可用的所有 Amazon Simple Email Service (Amazon SES) 聯絡人清單。 AWS 帳戶 | 2022 年 8 月 22 日 |
| AWS_ConfigRole – 新增 datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists | 此政策現在授予傳回 AWS DataSync 代理程式清單、DataSync 來源和目的地位置以及 DataSync 任務的權限 AWS 帳戶；列出與中一個或多個指定 AWS Cloud Map 命名空間關聯的命名空間和服務的摘要資訊 AWS 帳戶；並列出中可用的所有 Amazon Simple Email Service (Amazon SES) 聯絡人清單。 AWS 帳戶 | 2022 年 8 月 22 日 |
| ConfigConformsServ iceRolePolicy – 新增 cloudwatch:PutMetricData | 此政策現在授予將指標資料點發佈到 Amazon 的權限 CloudWatch。 | 2022 年 7 月 25 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio | 此政策現在支援 Amazon 彈性容器服務 (Amazon ECS)、Amazon、Amazon FSx、Amazon 管理服務 Apache Flink ElastiCache、Amazon 定位服務 EventBridge、Amazon 卡夫卡、Amazon Rekognition、Amazon 簡單儲存服務 (Amazon S3)、亞馬遜簡單電子郵件服務 (亞馬遜 SES)、亞馬遜管理串流 QuickSight、亞馬遜 Rekognition AWS RoboMaker、亞馬遜簡單儲存服務 (亞馬遜 S3)、亞馬遜簡單電子郵件服務 (亞馬遜 SES) AWS Amplify、亞馬遜管理串流 AWS AppConfig AWS AppSync AWS Billing Conductor、、AWS DataSync、、 AWS Firewall Manager、、 AWS Glue、、、、 AWS IAM Identity Center IAM Elastic Load Balancing。 | 2022 年 7 月 15 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| sso:GetInlinePolicyForPermissionSet | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De | 此政策現在支援 Amazon 彈性容器服務 (Amazon ECS)、Amazon、Amazon FSx、Amazon 管理服務 Apache Flink ElastiCache、Amazon 定位服務 EventBridge、Amazon 卡夫卡、Amazon Rekognition、Amazon 簡單儲存服務 (Amazon S3)、亞馬遜簡單電子郵件服務 (亞馬遜 SES)、亞馬遜管理串流 QuickSight、亞馬遜 Rekognition AWS RoboMaker、亞馬遜簡單儲存服務 (亞馬遜 S3)、亞馬遜簡單電子郵件服務 (亞馬遜 SES) AWS Amplify、亞馬遜管理串流 AWS AppConfig AWS AppSync AWS Billing Conductor、、AWS DataSync、、 AWS Firewall Manager、、 AWS Glue、、、、 AWS IAM Identity Center IAM Elastic Load Balancing。 | 2022 年 7 月 15 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| scribeLocationS3, datasync: DescribeLocationSmb, datasync:DescribeTask, datasync: ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVersions, imagebuilder: ListCompo | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| sso:GetInlinePolicyForPermissionSet | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De | 此政策現在授予取得指定 Amazon Athena 資料目錄清單、在 Athena 資料目錄中列出與 Athena 工作群組或資料目錄資源相關聯的標籤的權限；若要取得 Detective 行為圖形的清單 AWS 帳戶、取得指定 AWS Glue 開發端點名稱清單的資源中繼資料清單、取得有關指定開發端點的資訊、取得所有開發端點的資訊、取得指定開發端點的所有開發端點的資訊、取得所有 AWS Glue 開發端點的資訊 AWS 帳戶、取得指定 AWS Glue 開發端點的所有開發 AWS Glue 端點的資訊配置，獲取所有 AWS Glue 安全配置，獲取與 AWS Glue 資源關聯的標籤列表，獲取有關具有指定名稱的工作 AWS Glue 組的信息，檢索帳戶中所有 AWS Glue 搜索器資源的名稱，獲取一個中所有 AWS Glue `DevEndpoint` 資源的名稱 AWS 帳戶，列出一個 AWS 帳戶中所有 AWS Glue 作業資源的名稱 AWS 帳戶，獲取有關 AWS Glue 成員帳戶的詳細信息，列出在帳戶中創建的工作 AWS Glue 流程的名稱以及列出帳戶的可用 AWS Glue 工作組；擷取 Amazon GuardDuty 篩選 GuardDuty器的詳細資訊、擷 | 2022 年 5 月 31 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource | 取 GuardDuty IPSet、擷取集 GuardDutyThreatIntel合、擷取 GuardDuty 成員帳戶、取得篩選器清單、取得服務的 IPSet、擷取 GuardDuty 服務標籤，以及取得GuardDuty 服 GuardDuty 務；取得 Amazon Macie 帳戶的目前狀態和組態設定；擷取 AWS Resource Access Manager (AWS RAM) 資源共用的資源和主體關聯，以及擷取有關資源共用的詳細 AWS RAM 資訊； ThreatIntelSets 取得 Amazon Simple Email Service (Amazon SES) 現有組態集的相關資訊、取得與 Amazon SES 組態集關聯的事件目的地清單，以及列出與 Amazon SES 帳戶相關聯的所有組態集；若要取得身分中心目錄屬性清單，取得權限集的詳細資訊、取得指定 IAM 身分中心權限集的 IAM 受管政策、取得 IAM 執行個體許可集的詳細資訊 IAM 身分識別中心的標籤 AWS IAM Identity Center 資源。 | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De | 此政策現在授予取得指定 Amazon Athena 資料目錄清單、在 Athena 資料目錄中列出與 Athena 工作群組或資料目錄資源相關聯的標籤的權限；若要取得 Detective 行為圖形的清單 AWS 帳戶、取得指定 AWS Glue 開發端點名稱清單的資源中繼資料清單、取得有關指定開發端點的資訊、取得所有開發端點的資訊、取得指定開發端點的所有開發端點的資訊、取得所有 AWS Glue 開發端點的資訊 AWS 帳戶、取得指定 AWS Glue 開發端點的所有開發 AWS Glue 端點的資訊配置，獲取所有 AWS Glue 安全配置，獲取與 AWS Glue 資源關聯的標籤列表，獲取有關具有指定名稱的工作 AWS Glue 組的信息，檢索帳戶中所有 AWS Glue 搜索器資源的名稱，獲取一個中所有 AWS Glue `DevEndpoint` 資源的名稱 AWS 帳戶，列出一個 AWS 帳戶中所有 AWS Glue 作業資源的名稱 AWS 帳戶，獲取有關 AWS Glue 成員帳戶的詳細信息，列出在帳戶中創建的工作 AWS Glue 流程的名稱以及列出帳戶的可用 AWS Glue 工作組；擷取 Amazon GuardDuty 篩選 GuardDuty器的詳細資訊、擷 | 2022 年 5 月 31 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource | 取 GuardDuty IPSet、擷取集 GuardDutyThreatIntel合、擷取 GuardDuty 成員帳戶、取得篩選器清單、取得服務的 IPSet、擷取 GuardDuty 服務標籤，以及取得GuardDuty 服 GuardDuty 務；取得 Amazon Macie 帳戶的目前狀態和組態設定；擷取 AWS Resource Access Manager (AWS RAM) 資源共用的資源和主體關聯，以及擷取有關資源共用的詳細 AWS RAM 資訊； ThreatIntelSets 取得 Amazon Simple Email Service (Amazon SES) 現有組態集的相關資訊、取得與 Amazon SES 組態集關聯的事件目的地清單，以及列出與 Amazon SES 帳戶相關聯的所有組態集；若要取得身分中心目錄屬性清單，取得權限集的詳細資訊、取得指定 IAM 身分中心權限集的 IAM 受管政策、取得 IAM 執行個體許可集的詳細資訊 IAM 身分識別中心的標籤 AWS IAM Identity Center 資源。 | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies | 此原則現在授與取得所有或指定 AWS CloudTrail 事件資料存放區 (EDS) 相關資訊的權限、取得有關全部或指定 AWS CloudFormation 資源的資訊、取得 DynamoDB 加速器 (DAX) 參數群組或子網路群組的清單、取得有關 AWS Database Migration Service (AWS DMS) 目前存取區域中帳戶複寫工作的資訊，以及取得指定類型的所有原則清單。AWS Organizations | 2022 年 4 月 7 日 |
| AWS_ConfigRole – 新增 cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies | 此原則現在授與取得所有或指定 AWS CloudTrail 事件資料存放區 (EDS) 相關資訊的權限、取得有關全部或指定 AWS CloudFormation 資源的資訊、取得 DynamoDB 加速器 (DAX) 參數群組或子網路群組的清單、取得有關 AWS Database Migration Service (AWS DMS) 目前存取區域中帳戶複寫工作的資訊，以及取得指定類型的所有原則清單。AWS Organizations | 2022 年 4 月 7 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara | 此政策現在支援 DynamoDB 加速器 AWS Backup AWS Batch、Amazon DynamoDB AWS Database Migration Service、Amazon 彈性運算雲端 (Amazon EC2)、亞馬 Amazon Elastic Kubernetes Service、Amazon FSx、Amazon Relational Database Service 服務、V2 和 Amazon GuardDuty 的其他許可。 AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces | 2022 年 3 月 14 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces | | |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct | 此政策現在支援 DynamoDB 加速器 AWS Backup AWS Batch、Amazon DynamoDB AWS Database Migration Service、Amazon 彈性運算雲端 (Amazon EC2)、亞馬 Amazon Elastic Kubernetes Service、Amazon FSx、Amazon Relational Database Service 服務、V2 和 Amazon GuardDuty 的其他許可。 AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces | 2022 年 3 月 14 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces | | |
| AWSConfigServiceRolePolicy – 新增 elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies | 此政策現在授予權限，以取得有關 Elastic Beanstalk 環境的詳細資料以及指定 Elastic Beanstalk 組態集的設定說明、取得 OpenSearch 或 Elasticsearch 版本的對應、描述資料庫的可用 Amazon RDS 選項群組，以及取得有關部署組態的資訊。 CodeDeploy 此政策現在也授與權限，可擷取附加至某個 AWS 帳戶指定的替代聯絡人、擷取有關 AWS Organizations 政策的資訊、擷取 Amazon ECR 儲存庫政策、擷取存檔 AWS Config 規則的資訊、擷取 Amazon ECS 任務定義系列清單、列出指定子 OU 或帳戶的根或父組織單位 (OU)，以及列出附加到指定目標根、組織單位或帳戶的政策。 | 2022 年 2 月 10 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole – 新增 elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies | 此政策現在授予權限，以取得有關 Elastic Beanstalk 環境的詳細資料以及指定 Elastic Beanstalk 組態集的設定說明、取得 OpenSearch 或 Elasticsearch 版本的對應、描述資料庫的可用 Amazon RDS 選項群組，以及取得有關部署組態的資訊。 CodeDeploy 此政策現在也授與權限，可擷取附加至某個 AWS 帳戶指定的替代聯絡人、擷取有關 AWS Organizations 政策的資訊、擷取 Amazon ECR 儲存庫政策、擷取存檔 AWS Config 規則的資訊、擷取 Amazon ECS 任務定義系列清單、列出指定子 OU 或帳戶的根或父組織單位 (OU)，以及列出附加到指定目標根、組織單位或帳戶的政策。 | 2022 年 2 月 10 日 |
| AWSConfigServiceRolePolicy – 新增 logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent | 此政策現在授予建立 Amazon 日 CloudWatch 誌群組和串流的權限，以及將日誌寫入建立的日誌串流。 | 2021 年 12 月 15 日 |
| AWS_ConfigRole – 新增 logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent | 此政策現在授予建立 Amazon 日 CloudWatch 誌群組和串流的權限，以及將日誌寫入建立的日誌串流。 | 2021 年 12 月 15 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – 新增 es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots | 此政策現在授予取得 Amazon OpenSearch 服務 (服 OpenSearch 務) 網域/網域詳細資料的權限，以及取得特定 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫參數群組的詳細參數清單的權限。此政策還授予獲得有關 Amazon ElastiCache 快照詳細資訊的許可。 | 2021 年 9 月 8 日 |
| AWS_ConfigRole – 新增 es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots | 此政策現在授予取得 Amazon OpenSearch 服務 (服 OpenSearch 務) 網域/網域詳細資料的權限，以及取得特定 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫參數群組的詳細參數清單的權限。此政策還授予獲得有關 Amazon ElastiCache 快照詳細資訊的許可。 | 2021 年 9 月 8 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy— AWS 資源類型的新增logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine 和其他權限 | 此政策現在授予的許可，可列出日誌群組標籤、列出狀態機器標籤，以及列出所有狀態機器。此政策現在會授予可取得狀態機器詳細資訊的許可。該政策現在還支持 Amazon EC2 Systems Manager（SSM），Amazon 彈性容器註冊表，Amazon FSX，Amazon 數據火狐，阿帕奇卡夫卡 Amazon 託管流（Amazon MSK），Amazon Relational Database Service（Amazon RDS），Amazon 路線 53，Amazon 簡單通知服務 SageMaker，和。 AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway | 2021 年 7 月 28 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole— 新增 l ogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine 和 AWS 資源類型的其他權限 | 此政策現在授予的許可，可列出日誌群組標籤、列出狀態機器標籤，以及列出所有狀態機器。此政策現在會授予可取得狀態機器詳細資訊的許可。該政策現在還支持 Amazon EC2 Systems Manager（S SM），Amazon 彈性容器註冊表，Amazon FSX，Amazo n 數據火狐，阿帕奇卡夫卡 Amazon 託管流（Amazon MSK），Amazon Relationa l Database Service（A mazon RDS），Amazon 路線 53，Amazon 簡單通知服務 SageMaker，和。 AWS Database Migration Service A WS Global Accelerator AWS Storage Gateway | 2021 年 7 月 28 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSConfigServiceRolePolicy— 為 AWS 資源類型添加ssm:DescribeDocumentPermission和其他權限 | 此政策現在會授予可檢視 AWS Systems Manager 文件許可和 IAM Access Analyzer 相關資訊的許可。此政策現在支援 Amazon Kinesis、Amazon、Amazon EMR ElastiCache、亞馬遜路線 53 和 Amazon Relational Database Service 服務 (Amazon RDS) 的其他 AWS 資源類型。 AWS Network Firewall這些權限變更 AWS Config 允許叫用支援這些資源類型所需的唯讀 API。此原則現在也支援針對 vpc 內 AWS Config 部受管規則篩選 Lambda @Edge 函數。 | 2021 年 6 月 8 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole— 為 AWS 資源類型添加ssm:DescribeDocumentPermission和其他權限 | 此政策現在會授予可檢視 AWS Systems Manager 文件許可和 IAM Access Analyzer 相關資訊的許可。此政策現在支援 Amazon Kinesis、Amazon、Amazon EMR ElastiCache、亞馬遜路線 53 和 Amazon Relational Database Service 服務 (Amazon RDS) 的其他 AWS 資源類型。 AWS Network Firewall這些權限變更 AWS Config 允許叫用支援這些資源類型所需的唯讀 API。此原則現在也支援針對 vpc 內 AWS Config 部受管規則篩選 Lambda @Edge 函數。 | 2021 年 6 月 8 日 |
| AWSConfigServiceRolePolicy - 新增可向 API Gateway 發出唯讀 GET 呼叫的 apigateway:GET 許可，以及可調用 Amazon S3 唯讀 API 的 s3:GetAccessPointPolicy 許可和 s3:GetAccessPointPolicyStatus 許可 | 此原則現在會授與允許 AWS Config 對 API Gateway 進行唯讀 GET 呼叫以支援 API Gateway AWS Config 規則的權限。該政策還新增許可，AWS Config 允許叫用 Amazon Simple Storage Service (Amazon S3) 唯讀 API，這些 API 是支援新`AWS::S3::AccessPoint` 資源類型所需的。 | 2021 年 5 月 10 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ ConfigRole — 新增apigateway:GET對 API Gateway 進行唯讀 GET 呼叫的s3:GetAccessPointPolicy權限，以及叫用 Amazon S3 唯讀 API 的s3:GetAccessPoint PolicyStatus許可和許可 | 此原則現在授與允 AWS Config 許 AWS Config 對 API Gateway 進行唯讀 GET 呼叫以支援 API Gateway 的權限。該政策還新增許可，AWS Config 允許叫用 Amazon Simple Storage Service (Amazon S3) 唯讀 API，這些 API 是支援新`AWS::S3::AccessPoint` 資源類型所需的。 | 2021 年 5 月 10 日 |
| AWSConfigServiceRolePolicy— 為 AWS 資源類型添加ssm:ListDocuments權限和其他權限 | 此政策現在會授予可檢視 AWS Systems Manager 指定文件相關資訊的許可。此政策現在還支援 Amazon 彈性檔案系統 AWS Backup、Amazon、Amazon 簡單儲存服務 (Amazon S3) ElastiCache、亞馬遜彈性運算雲 (Amazon EC2)、亞馬遜 Kinesis、亞馬遜和亞馬遜 SageMaker路線 53 的其他 AWS 資源類型。 AWS Database Migration Service這些權限變更 AWS Config 允許叫用支援這些資源類型所需的唯讀 API。 | 2021 年 4 月 1 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS_ConfigRole— 為 AWS 資源類型添加ssm:ListDocuments權限和其他權限 | 此政策現在會授予可檢視 AWS Systems Manager 指定文件相關資訊的許可。此政策現在還支援 Amazon 彈性檔案系統 AWS Backup、Amazon、Amazon 簡單儲存服務 (Amazon S3) ElastiCache、亞馬遜彈性運算雲 (Amazon EC2)、亞馬遜 Kinesis、亞馬遜和亞馬遜 SageMaker路線 53 的其他 AWS 資源類型。 AWS Database Migration Service這些權限變更 AWS Config 允許叫用支援這些資源類型所需的唯讀 API。 | 2021 年 4 月 1 日 |
| `AWSConfigRole` 已棄用 | `AWSConfigRole` 已棄用。替換政策是 `AWS_ConfigRole` 。 | 2021 年 4 月 1 日 |
| AWS Config 開始追蹤變更 | AWS Config 開始追蹤其 AWS 受管理策略的變更。 | 2021 年 4 月 1 日 |

## 指派給的 IAM 角色的許可 AWS Config

IAM 角色可讓您定義一組許可。 AWS Config 假設您指派給它的角色，以寫入 S3 儲存貯體、發佈到 SNS 主題，以及發出`Describe`或 `List` API 請求以取得 AWS 資源的組態詳細資料。如需 IAM 角色的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 角色。

當您使用 AWS Config 主控台建立或更新 IAM 角色時， AWS Config 會自動為您附加必要的許可。如需詳細資訊，請參閱 使用主控 AWS Config 台進行設定。

內容


- 建立 IAM 角色 政策
  - 將 IAM 信任政策新增至您的角色

- 適用於 S3 儲存貯體的 IAM 角色政策
- 適用於 KMS Key 的 IAM 角色政策
- 適用於 Amazon SNS 主題的 IAM 角色政策
- 用以取得組態詳細資訊的 IAM 角色政策
- 管理 S3 儲存貯體記錄的許可

## 建立 IAM 角色 政策

當您使用主 AWS Config 控台建立 IAM 角色時， AWS Config 會自動為您附加所需的權限至該角色。

如果您使用進行設 AWS CLI 定 AWS Config 或正在更新現有 IAM 角色，則必須手動更新政策以允許 AWS Config 存取 S3 儲存貯體、發佈到 SNS 主題，以及取得有關資源的組態詳細資訊。

將 IAM 信任政策新增至您的角色

您可以建立 IAM 信任政策，以 AWS Config 便擔任角色並使用它來追蹤您的資源。如需有關信任政策的詳細資訊，請參閱《IAM 使用者指南》中的《角色術語和概念》。

以下是 AWS Config 角色的信任原則範例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

您可以使用上述 IAM 角色信任關係中的 `AWS:SourceAccount` 條件，限制 Config 服務主體在代表特定帳戶執行操作時，僅能與 AWS IAM 角色互動。

AWS Config 也支援限制 `AWS:SourceArn` Config 服務主體在代表擁有帳戶執行作業時僅承擔 IAM 角色的條件。使用 AWS Config 服務主體時，`AWS:SourceArn`屬性一律會設定為`arn:aws:config:sourceRegion:sourceAccountID:*`組態記錄程式的區域，而且`sourceAccountID`是包含組態記錄程式的帳戶識別碼。`sourceRegion`如需 AWS Config 組態錄製程式的詳細資訊，請參閱管理組態錄製程式。例如，新增下列條件以限制 Config 服務主體在代表帳戶 `123456789012` 在 `us-east-1` 區域中的組態記錄器 `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}` 時，僅能擔任 IAM 角色。

適用於 S3 儲存貯體的 IAM 角色政策

下列範例政策授 AWS Config 予存取 S3 儲存貯體的權限：

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::myBucketName"
    }
  ]
}
```

適用於 KMS Key 的 IAM 角色政策

下列範例政策授 AWS Config 予在 S3 儲存貯體交付的新物件上使用 KMS 型加密的權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

適用於 Amazon SNS 主題的 IAM 角色政策

下列範例原則 AWS Config 授與存取 SNS 主題的權限：

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

如果您的 SNS 主題已按照其他設定指示加密，請參閱《Amazon Simple Notification Service 開發人員指南》中的《設定 AWS KMS 許可》。

用以取得組態詳細資訊的 IAM 角色政策

若要記錄您的 AWS 資源組態， AWS Config 需要 IAM 許可以取得有關資源的組態詳細資料。

使用受 AWS 管政策 AWS_ ConfigRole 並將其附加到您指派給的 IAM 角色。 AWS Config AWS 每次新 AWS Config 增 AWS 資源類型支援時，都 AWS Config 會更新此原則，這表示只要角色已附加此受管理原則，就會繼續擁有取得組態詳細資料所需的權限。

如果您使用主控台建立或更新角色，請ConfigRole為您 AWS Config 附加 AWS_。

如果您使用 AWS CLI，請使用命`attach-role-policy`令並為 AW ConfigRole S_ 指定 Amazon 資源名稱 (ARN)：

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
```

### 管理 S3 儲存貯體記錄的許可

AWS Config 在建立、更新或刪除 S3 儲存貯體時記錄並傳送通知。

建議您使用 `AWSServiceRoleForConfig` (請參閱《使用 AWS Config的服務連結角色》) 或利用 `AWS_ConfigRole` 受管政策的自訂 IAM 角色。如需組態記錄最佳實務的詳細資訊，請參閱《AWS Config 最佳實務》。

如果您需要管理儲存貯體記錄的物件層級許可，請確保在 S3 儲存貯體政策中提供 `config.amazonaws.com` ( AWS Config 服務主體名稱) 對`AWS_ConfigRole`受管政策中所有 S3 相關許可的存取權。如需詳細資訊，請參閱《Amazon S3 儲存貯體許可》。

## 更新指派給的 IAM 角色 AWS Config

您可以隨時更新假設 AWS Config 的 IAM 角色。請在更新 IAM 角色前，確認您已建立新的角色來取代舊的角色。您必須將原則附加至新角色，以授與記錄組態 AWS Config 的權限，並將其傳遞至您的傳遞管道。此外，請務必複製新 IAM 角色的 Amazon Resource Name (ARN)。您會需要該項目來更新 IAM 角色。如需建立 IAM 角色並將必要政策連接至 IAM 角色的資訊，請參閱《建立 IAM 角色》。

> **Note**
>
> 若要尋找現有 IAM 角色的 ARN，請前往位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。在導覽窗格中，選擇 Roles (角色)。然後選擇需要角色的名稱，並在 Summary (摘要) 頁面的頂端尋找 ARN。

### 更新 IAM 角色

您可以使用 AWS Management Console 或更新您的 IAM 角色 AWS CLI。

To update the IAM role (Console)

如果您 AWS Config 在支援 AWS Config 規則的區域中使用，請完成以下步驟。如需支援區域的清單，請參閱《Amazon Web Services 一般參考》中的 AWS Config 區域與端點。

1. 請登入 AWS Management Console 並開啟 AWS Config 主控台，網址為 https://console.aws.amazon.com/config/。
2. 在導覽窗格中選擇 Settings (設定)。
3. 在「設定」頁面上選擇 「編輯」。
4. 在「資料控管」區段中，選擇下列項目的 IAM 角色 AWS Config：
   - 使用現有的 AWS Config 服務連結角色 — AWS Config 建立具有所需權限的角色。
   - 從您的帳戶中選擇角色 — 對於現有角色，請在帳戶中選擇 IAM 角色。
5. 選擇儲存。

To update the IAM role (AWS CLI)

使用 `put-configuration-recorder` 命令並指定新角色的 Amazon Resource Name (ARN)：

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

## 適用於 AWS Config 交付通道的 Amazon S3 儲存貯體的許可

> **Important**
> 本頁是關於為 AWS Config 交付通道設定 Amazon S3 儲存貯體的相關資訊。此頁面與 AWS Config 組態記錄程式可記錄的`AWS::S3::Bucket`資源類型無關。如需有關 AWS Config 傳遞管道的詳細資訊，請參閱管理傳遞管道。

根據預設，所有 Amazon S3 儲存貯體和物件皆為私有。只有建立值區的資源擁有者才能存取該值區。AWS 帳戶 然而，資源擁有者可以選擇將存取許可授予其他使用者和資源。執行此作業的其中一種方式便是撰寫存取政策。

如果自動為您 AWS Config 建立 Amazon S3 儲存貯體 (例如，如果您使用 AWS Config 主控台設定交付通道)，這些許可會自動新增至 Amazon S3 儲存貯體。但是，若您指定現有的 Amazon S3 儲存貯體，您必須確認該 S3 儲存貯體具有正確的許可。

> **Note**
>
> 物件不會繼承其儲存貯體的許可。例如，若您建立儲存貯體，並將寫入存取授予使用者，除非使用者明確授予存取權給您，否則您無法存取該使用者的物件。

內容


- 使用 IAM 角色時的 Amazon S3 儲存貯體必要許可
- 使用服務連結角色時的 Amazon S3 儲存貯體必要許可
- 授予對 Amazon S3 儲 AWS Config 存貯體的存取權


## 使用 IAM 角色時的 Amazon S3 儲存貯體必要許可

AWS Config 將組態資訊 (歷程檔案和快照) 傳送到帳戶中的 Amazon S3 儲存貯體時，它會擔任您在設定時指派的 IAM 角色 AWS Config。當 AWS Config 將組態資訊傳送至另一個帳戶中的 Amazon S3 儲存貯體時，會先嘗試使用 IAM 角色，但若儲存貯體的存取政策並未將 `WRITE` 存取權授予 IAM 角色，則此嘗試便會失敗。在這種情況下，再次 AWS Config 發送信息，這次作為 AWS Config 服務主體。在傳遞成功之前，存取原則必須授與`config.amazonaws.com`主體名稱的`WRITE`存取權。 AWS Config 那麼是它交付給 S3 存儲桶的對象的所有者。您必須將下文步驟 6 所提及的存取政策連接至位於另一個帳戶中的 Amazon S3 儲存貯體，將 AWS Config 存取權授予 Amazon S3 儲存貯體。

之前 AWS Config 可以將日誌交付到 Amazon S3 儲存貯體，請 AWS Config 檢查儲存貯體是否存在以及儲存貯體所在的 AWS 區域。 AWS Config 嘗試呼叫 Amazon S3 HeadBucketAPI 以檢查儲存貯體是否存在並取得儲存貯體區域。如果在執行位置檢查時未提供尋找值區的權限，您會在 AWS CloudTrail 記錄中看到`AccessDenied`錯誤。不過，如果您並未提供儲存貯體位置許可，日誌仍會成功傳遞至您的 Amazon S3 儲存貯體。

> **Note**
>
> 若要允許 Amazon S3 `HeadBucket` API 的許可，請提供可以 Sid `AWSConfigBucketExistenceCheck` 身分執行 `s3:ListBucket` 動作的許可，如下文步驟 6 所述。

## 使用服務連結角色時的 Amazon S3 儲存貯體必要許可

AWS Config 服務連結角色沒有將物件放入 Amazon S3 儲存貯體的權限。因此，如果您 AWS Config 使用服務連結角色進行設定，則 AWS Config 會改為傳送組態項目做為 AWS Config 服務主體。您需要將下面步驟 6 中提到的存取政策附加到您自己帳戶或其他帳戶中的 Amazon S3 儲存貯體，以授予對 Amazon S3 儲 AWS Config 存貯體的存取權。

## 授予對 Amazon S3 儲 AWS Config 存貯體的存取權

請遵循下列步驟，將存取政策新增至您自己帳戶或另一個帳戶中的 Amazon S3 儲存貯體。存取政策允許 AWS Config 將組態資訊傳送到 Amazon S3 儲存貯體。

1. AWS Management Console 使用具有 S3 儲存貯體的帳戶登入。
2. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
3. 選取您要用 AWS Config 來傳送組態項目的值區，然後選擇 [內容]。
4. 選擇許可。
5. 選擇 Edit Bucket Policy (編輯儲存貯體政策)。
6. 將下列政策複製到 Bucket Policy Editor (儲存貯體政策編輯器) 視窗：

> **Important**
>
> 作為允許 AWS Config 存取 Amazon S3 儲存貯體時的安全性最佳實務，我們強烈建議您以`AWS:SourceAccount`條件限制儲存貯體政策中的存取。如果您現有的儲存貯體政策未遵循此安全最佳作法，強烈建議您編輯該儲存貯體政策以納入此保護。這可確 AWS Config 保僅代表預期的使用者授予存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName",
```

```
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

> **Note**
>
> 將權限授予 IAM 角色而非 AWS Config 服務主體名稱 (SPN) 時，請確保您的 IAM 角色具有跨帳戶儲存貯體的`PutObjectACL`權限，以避免權限不足錯誤。請參閱《適用於 S3 儲存貯體的 IAM 角色政策》一文中的 IAM 角色政策範例。

7. 取代儲存貯體政策中的下列數值：
   - *## BucketName* — AWS Config 將交付組態項目的 Amazon S3 儲存貯體的名稱。
   - *[##] ##* - Amazon S3 物件金鑰的選用新增項目，有助於在儲存貯體中建立類似資料夾的組織。
   - *#### ID* — AWS Config 將會將組態項目傳送至目標儲存貯體的帳戶識別碼。
8. 選擇 Save (儲存) 然後 Close (關閉)。

您可以使用上述 Amazon S3 儲存貯體政策中的 `AWS:SourceAccount` 條件，限制 Config 服務主體在代表特定帳戶執行操作時，僅能與 Amazon S3 儲存貯體互動。如果您計劃在同一組織的多個帳戶 AWS Config 中進行設定，以便將組態項目交付到單一 Amazon S3 儲存貯體，我們建議您使用 IAM 角色而不是服務連結角色，以便您可以使用諸如`AWS:PrincipalOrgID`此類的 AWS Organizations 條件金鑰。如需管理要搭配使用之 IAM 角色存取權限的詳細資訊 AWS Config，請參閱指派給的 IAM 角色的許可 AWS Config。如需有關管理的存取權限的詳細資訊 AWS Organizations，請參閱管理 AWS 組織的存取權限。

AWS Config 此外，也支援限制 `AWS:SourceArn` Config 服務主體在代表特定 AWS Config 交付通道執行操作時僅與 Amazon S3 儲存貯體互動的條件。使用 AWS Config 服務主體時，`AWS:SourceArn`屬性一律會設定為`arn:aws:config:sourceRegion:sourceAccountID:*`傳遞通道的區域，而且`sourceAccountID`是包含傳遞通道之帳戶的 ID。`sourceRegion`如需有關 AWS Config 傳送管道的詳細資訊，請參閱管理傳遞管道。例如，新增下列條件以限制 Config 服務主體在代表帳戶 `123456789012` 在 `us-east-1` 區域中的交付通道 `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}` 時，僅能與 Amazon S3 儲存貯體互動。

## AWS Config 傳遞管道的 KMS 金鑰權限

如果您想要為 S3 儲存貯體的 AWS KMS 金鑰建立政策，以便在 S3 儲存貯體交付所交付的物件上使用 KMS 型加密，請使用本主題中 AWS Config 的資訊。

內容

- 使用 IAM 角色時的 KMS Key 必要許可 (S3 儲存貯體交付)
- 使用服務連結角色時 AWS KMS 金鑰的必要權限 (S3 儲存貯體交付)
- 授與 AWS KMS 金鑰 AWS Config 存取權

## 使用 IAM 角色時的 KMS Key 必要許可 (S3 儲存貯體交付)

如果您 AWS Config 使用 IAM 角色進行設定，則可以將遵循權限政策附加到 KMS 金鑰：

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> 如果 IAM 角色、Amazon S3 儲存貯體政策或 AWS KMS 金鑰未提供適當的存取權限 AWS Config，則 AWS Config嘗試將組態資訊傳送到 Amazon S3 儲存貯體將會失敗。在這種情況下，再次 AWS Config 發送信息，這次作為 AWS Config 服務主體。在這種情況下，您必須將權限政策 (如下所述) 附加至 AWS KMS 金鑰，以便在將資訊傳送到 Amazon S3 儲 AWS Config 存貯體時授予使用金鑰的存取權。

## 使用服務連結角色時 AWS KMS 金鑰的必要權限 (S3 儲存貯體交付)

AWS Config 服務連結角色沒有存取 AWS KMS 金鑰的權限。因此，如果您 AWS Config 使用服務連結角色進行設定，則 AWS Config 會改為以 AWS Config 服務主體的身分傳送資訊。您需要將存取政策 (如下所述) 附加至 AWS KMS 金鑰，才能在將資訊傳送至 Amazon S3 儲 AWS Config 存貯體時授予使用 AWS KMS 金鑰的存取權。

## 授與 AWS KMS 金鑰 AWS Config 存取權

此政策允許在 AWS Config 將資訊傳送到 Amazon S3 儲存貯體時使用 AWS KMS 金鑰

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

替換金鑰政策中的下列值：

- *MyKMSkeyarn* — 用於將交付組態項目的 Amazon S3 儲存貯體中資料加密的 AWS KMS 金鑰的 AWS Config ARN。
- *sourceAccountID* - 帳戶 ID， AWS Config 會為其交付組態項目。

您可以使用上述 AWS KMS 金鑰原則中的`AWS:SourceAccount`條件，限制 Config 服務主體在代表特定帳戶執行作業時僅與 AWS KMS 金鑰互動。

AWS Config 此外，也支援限制 `AWS:SourceArn` Config 服務主體在代表特定 AWS Config 交付通道執行操作時僅與 Amazon S3 儲存貯體互動的條件。使用 AWS Config 服務主體時，`AWS:SourceArn`屬性一律會設定為`arn:aws:config:sourceRegion:sourceAccountID:*`傳遞通道的區域，而且`sourceAccountID`是包含傳遞通道之帳戶的 ID。`sourceRegion`如需有關 AWS Config 傳送管道的詳細資訊，請參閱管理傳遞管道。例如，新增下列條件以限制 Config 服務主體在代表帳戶 `123456789012` 在 `us-east-1` 區域中的交付通道 `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}` 時，僅能與 Amazon S3 儲存貯體互動。

## Amazon SNS 主題的許可

本主題說明如何設定 AWS Config 以交付不同帳戶擁有的 Amazon SNS 主題。 AWS Config 必須具有必要的許可才能將通知傳送到 Amazon SNS 主題。對於相同帳戶設定，當主 AWS Config 控台建立 Amazon SNS 主題或從自己的帳戶選擇 Amazon SNS 主題時，請 AWS Config 確保 Amazon SNS 主題包含必要的許可並遵循安全最佳實務。

> **Note**
>
> AWS Config 目前僅支援相同區域和跨帳戶的存取。用於修復 AWS Systems Manager (SSM) 文件或記錄器傳遞通道的 SNS 主題不能跨區域。

內容


- 使用 IAM 角色時的 Amazon SNS 主題必要許可
- 使用服務連結角色時的 Amazon SNS 主題必要許可
- 授 AWS Config 予對 Amazon SNS 主題的存取權。
- Amazon SNS 主題故障診斷


### 使用 IAM 角色時的 Amazon SNS 主題必要許可

您可以將許可政策連接到其他帳戶擁有的 Amazon SNS 主題。如果想要使用其他帳戶的 Amazon SNS 主題，請務必將下列政策連接至現有的 Amazon SNS 主題。

```
{
```

```
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

對 `Resource` 金鑰而言，*`account-id`* 是主題擁有者的 AWS 帳戶編號。對於*`## ID1`*、*`## ID2 ## #-id 3`*，請使用將資料傳送至 Amazon SNS 主題 AWS 帳戶 的。您可將 *`region`* 和 *`myTopic`* 替換為適當的值。

AWS Config 傳送通知給 Amazon SNS 主題時，會先嘗試使用 IAM 角色，但如果角色或 AWS 帳戶 沒有發佈到主題的權限，則此嘗試會失敗。在此情況下， AWS Config 會再次傳送通知，這次會以 AWS Config 服務主體名稱 (SPN) 的形式傳送。發布成功之前，主題的存取政策必須授與 `config.amazonaws.com` 主體名稱的 `sns:Publish` 存取權。如果 IAM 角色無權向主題發布通知，您必須將存取政策 (下節說明) 連接至 Amazon SNS 主題，才能授權 AWS Config 存取 Amazon SNS 主題。

## 使用服務連結角色時的 Amazon SNS 主題必要許可

AWS Config 服務連結角色沒有存取 Amazon SNS 主題的權限。因此，如果您 AWS Config 使用服務連結角色 (SLR) 進行設定，則 AWS Config 會改為以 AWS Config 服務主體的身分傳送資訊。您需要將存取政策 (如下所述) 附加至 Amazon SNS 主題，才能授予將資訊傳送至 Amazon SNS 主題的 AWS Config 存取權。

在相同帳戶設定中，當 Amazon SNS 主題和 SLR 位於同一帳戶，且 Amazon SNS 政策授予 SLR `"sns:Publish"` 許可時，您不需要使用 AWS Config SPN。以下許可政策和安全性最佳實務建議適用於跨帳戶設定。

## 授 AWS Config 予對 Amazon SNS 主題的存取權。

此政策 AWS Config 允許傳送通知給 Amazon SNS 主題。若要授與其他帳戶 AWS Config 存取 Amazon SNS 主題的權限，您需要附加以下許可政策。

> **Note**
>
> 作為安全性最佳作法，強烈建議您確定只能透過限制 AWS Config 對`AWS:SourceAccount`條件中列出之帳戶的存取權限，以代表預期的使用者存取資源。

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

對 `Resource` 金鑰而言，*`account-id`* 是主題擁有者的 AWS 帳戶編號。對於*`## ID1`*、*`## ID2 ## #-id 3`*，請使用將資料傳送至 Amazon SNS 主題 AWS 帳戶 的。您可將 *`region`* 和 *`myTopic`* 替換為適當的值。

您可以使用先前 Amazon SNS 主題政策中的`AWS:SourceAccount`條件，限制 AWS Config 服務主體名稱 (SPN) 在代表特定帳戶執行操作時僅與 Amazon SNS 主題互動。

AWS Config 也支援限制 AWS Config 服務主體名稱 (SPN) 在代表特定 AWS Config 交付通道執行操作時僅與 S3 儲存貯體互動的`AWS:SourceArn`條件。使用 AWS Config 服務主體名稱 (SPN) 時，`AWS:SourceArn`屬性一律會設定為`arn:aws:config:sourceRegion:sourceAccountID:*`傳遞通道的 [區域]，並且`sourceAccountID`是包含傳遞通道之帳戶的 ID。`sourceRegion`如需有關 AWS Config 傳送管道的詳細資訊，請參閱管理傳遞管道。例如，新增下列條件以限制 AWS Config 服務主體名稱 (SPN) 僅代表帳戶中`us-east-1`區域中的交付通道與 S3 儲存貯體互動`123456789012`：`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

### Amazon SNS 主題故障診斷

AWS Config 必須具有傳送通知至 Amazon SNS 主題的權限。如果 Amazon SNS 主題無法收到通知，請確認假設的 IAM 角色具有必要的`sns:Publish`許可。 AWS Config

## 疑難排解 AWS Config 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 AWS Config 常見問題。

主題

- 我沒有執行操作的授權 AWS Config
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪 AWS 帳戶 問我的 AWS Config 資源

### 我沒有執行操作的授權 AWS Config

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在`mateojackson` IAM 使用者嘗試使用主控台檢視一個虛構 *`my-example-widget`* 資源的詳細資訊，但卻無虛構 `config:`*`GetWidget`* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 Mateo 政策，允許他使用 `config:`*`GetWidget`* 動作存取 *`my-example-widget`* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我沒有授權執行 iam：PassRole

如果您收到錯誤，告知您未獲授權執行 `iam:PassRole` 動作，您的政策必須更新，允許您將角色傳遞給 AWS Config。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 AWS Config中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我想允許我以外的人訪 AWS 帳戶 問我的 AWS Config 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS Config 支援這些功能，請參閱如何與 IAM AWS Config 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

# 使用服務連結角色 AWS Config

AWS Config 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結到 AWS Config的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Config 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS Config 更輕鬆地設定，因為您不需要手動新增必要的權限。 AWS Config 定義其服務連結角色的權限，除非另有定義，否則只 AWS Config 能擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

## 的服務連結角色權限 AWS Config

AWS Config 使用名為的服務連結角色 AWSServiceRoleForConfig— AWS Config 使用此服務連結角色代表您呼叫其他 AWS 服務。

服AWSServiceRoleForConfig務連結角色會信任`config.amazonaws.com`服務擔任該角色。

`AWSServiceRoleForConfig`角色的權限原則包含 AWS Config 資源的唯讀和唯寫權限，以及其他支援之服務中資源的 AWS Config 唯讀權限。如果要檢視受管理的策略 AWSServiceRoleForConfig，請參閱的AWS 受管政策 AWS Config。如需詳細資訊，請參閱 支援的資源類型。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

若要在中使用服務連結角色 AWS Config，您必須在 Amazon S3 儲存貯體和 Amazon SNS 主題上設定許可。如需詳細資訊，請參閱使用服務連結角色時的 Amazon S3 儲存貯體必要許可、使用服務連結角色時 AWS KMS 金鑰的必要權限 (S3 儲存貯體交付)及使用服務連結角色時的 Amazon SNS 主題必要許可。

## 建立下列項目的服務連結角色 AWS Config

在 IAM CLI 或 IAM API 中，建立一個使用 `config.amazonaws.com` 服務名稱的服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立服務連結角色。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

### 編輯下列項目的服務連結角色 AWS Config

AWS Config 不允許您編輯AWSServiceRoleForConfig服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

### 刪除下列項目的服務連結角色 AWS Config

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 當您嘗試刪除資源時，如果 AWS Config 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要刪除使用的 AWS Config 資源 AWSServiceRoleForConfig

請確定您沒有使用服務連結角色的 `ConfigurationRecorders`。您可以使用 AWS Config 控制台停止配置記錄器。若要停止記錄，請在 Recording is on (記錄已開啟) 下方選擇 Turn off (關閉)。

您可以刪除`ConfigurationRecorder`使用 AWS Config API。若要刪除，請使用 `delete-configuration-recorder` 命令。

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 AWSServiceRoleForConfig服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

## 中的事件回應 AWS Config

安全性是最高的優先事項 AWS。作為 AWS 雲端共同責任模式的一部分，您可以 AWS 管理符合最敏感安全性組織需求的資料中心、網路和軟體架構。 AWS 負責與 AWS Config 服務本身相關的任何事件

響應。此外，身為 AWS 客戶，您有責任維護雲端中的安全性。這表示您可以透過可存取的 AWS 工具和功能來控制選擇實作的安全性，並負責共用責任模型中的事件回應。

透過為雲端中執行的應用程式建立符合目標的安全性基準，您可以偵測可以回應的偏差。由於安全性事件回應可能是一個複雜的主題，因此我們建議您檢閱下列資源，以便更了解事件回應 (IR) 和您的選擇對公司目標的影響：AWS 安全性事件回應指南、AWS 安全性最佳實務白皮書，以及AWS 雲端採用架構 (CAF) 白皮 paper 的安全性觀點。

## 符合性驗證 AWS Config

協力廠商稽核人員會評估其安全性與合規性， AWS Config 做為多個 AWS 合規計畫的一部分。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。

- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

# 韌性 AWS Config

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

# 基礎架構安全性 AWS Config

作為託管服務， AWS Config 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS Config 過網路進行存取。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

## 組態與漏洞分析

對於 AWS Config， AWS 處理基本安全性工作，例如客體作業系統 (OS) 和資料庫修補、防火牆組態和嚴重損壞修復。

# 預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源策略中使用`aws:SourceArn`和`aws:SourceAccount`全域條件前後關聯索引鍵，以限制將其他服務 AWS Config 提供給資源的權限。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 `aws:SourceArn`。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 `aws:SourceAccount`。

防範混淆代理人問題的最有效方法是使用 `aws:SourceArn` 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 `aws:SourceArn` 全域內容條件索引鍵搭配萬用字元 (*) 來表示 ARN 的未知部分。例如 `arn:aws:servicename:*:123456789012:*`。

如果 `aws:SourceArn` 值不包含帳戶 ID (例如 Amazon S3 儲存貯體 ARN)，您必須使用這兩個全域條件內容索引鍵來限制許可。

下列範例顯示如何在中使用`aws:SourceArn`和`aws:SourceAccount`全域條件上下文金鑰 AWS Config 來避免混淆的副問題：授與 Amazon S3 儲 AWS Config 存貯體的存取權。

# 安全性最佳做法 AWS Config

AWS Config 在您開發和實作自己的安全性原則時，提供許多安全性功能供您考量。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

- 運用標記功能 AWS Config，讓管理、搜尋和篩選資源變得更加容易。
- 確認您的傳送管道已正確設定，一旦確認，請確認 AWS Config 是否正確錄製。

如需詳細資訊，請參閱《AWS Config 最佳實務》部落格。

# 登錄和監控 AWS Config

AWS Config 與 (提供中使用者 AWS CloudTrail、角色或服務所採取之動作記錄的 AWS 服務) 整合 AWS Config。監控是維持 AWS 解決方案的可靠性、可用性和效能的 AWS Config 重要組成部分。

主題


- 使用記錄 AWS Config API 呼叫 AWS CloudTrail
- 監控


## 使用記錄 AWS Config API 呼叫 AWS CloudTrail

CloudTrail 擷取 AWS Config 作為事件的所有 API 呼叫。擷取的呼叫包括來自 AWS Config 主控台的呼叫和 AWS Config API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 AWS Config. 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出的要求 AWS Config、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

主題


- AWS Config 信息在 CloudTrail
- 瞭解 AWS Config 記錄檔項目
- 範例日誌檔案


### AWS Config 信息在 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動發生在中時 AWS Config，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在您的. 中檢視、搜尋和下載最近的活動 AWS 帳戶。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

對於您的事件的持續記錄 AWS 帳戶，包括事件 AWS Config，請創建一個跟踪。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail記錄檔

所有 AWS Config 操作均由 API 參考記錄 CloudTrail 並記錄在 AWS Config API 參考中。例如，呼叫「DeliverConfig快照」、「DeleteDelivery通道」和「通DescribeDelivery道」作業會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

## 瞭解 AWS Config 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

## 範例日誌檔案

如需 CloudTrail 記錄項目的範例，請參閱下列主題。

DeleteDeliveryChannel

以下是「DeleteDelivery通道」作業的範例 CloudTrail 記錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## DeliverConfigSnapshot

以下是DeliverConfig快照作業的範例 CloudTrail 記錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
```

```
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

## DescribeConfigurationRecorderStatus

以下是作DescribeConfigurationRecorderStatus業的範例 CloudTrail 記錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
```

```
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

以下是「 CloudTrail 記錄器」作業的範例DescribeConfiguration記錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

以下是「DescribeDelivery通道」作業的範例 CloudTrail 記錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## GetResourceConfigHistory

以下是作GetResourceConfigHistory業的範例 CloudTrail 記錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
```

```
        },
        "eventTime": "2014-12-11T00:58:42Z",
        "eventSource": "config.amazonaws.com",
        "eventName": "GetResourceConfigHistory",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "10.24.34.0",
        "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
        "requestParameters": {
          "resourceId": "vpc-a12bc345",
          "resourceType": "AWS::EC2::VPC",
          "limit": 0,
          "laterTime": "Dec 11, 2014 12:58:42 AM",
          "earlierTime": "Dec 10, 2014 4:58:42 PM"
        },
        "responseElements": null,
        "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
        "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
        "eventType": "AwsApiCall",
        "recipientAccountId": "111111111111"
        }
```

## PutConfigurationRecorder

以下是「錄製程式」作業的範例 CloudTrail 記PutConfiguration錄檔。

```
{
        "eventVersion": "1.02",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::222222222222:user/JohnDoe",
          "accountId": "222222222222",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName": "JohnDoe"
        },
        "eventTime": "2014-12-11T18:35:23Z",
        "eventSource": "config.amazonaws.com",
        "eventName": "PutConfigurationRecorder",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
        "requestParameters": {
          "configurationRecorder": {
            "name": "default",
```

```
            "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
          }
        },
        "responseElements": null,
        "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
        "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
        "eventType": "AwsApiCall",
        "recipientAccountId": "222222222222"
      }
```

## PutDeliveryChannel

以下是「PutDelivery通道」作業的範例 CloudTrail 記錄檔。

```
{
        "eventVersion": "1.02",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::222222222222:user/JohnDoe",
          "accountId": "222222222222",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName": "JohnDoe"
        },
        "eventTime": "2014-12-11T18:33:08Z",
        "eventSource": "config.amazonaws.com",
        "eventName": "PutDeliveryChannel",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
        "requestParameters": {
          "deliveryChannel": {
            "name": "default",
            "s3BucketName": "config-api-test-pdx",
            "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
          }
        },
        "responseElements": null,
        "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
        "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
        "eventType": "AwsApiCall",
        "recipientAccountId": "222222222222"
      }
```

## StartConfigurationRecorder

以下是「錄製程式」作業的範例 CloudTrail 記StartConfiguration錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## StopConfigurationRecorder

以下是「錄製程式」作業的範例 CloudTrail 記StopConfiguration錄檔。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
```

```
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

# 監控

您可以使用其他 AWS 服務來監視 AWS Config 資源。

- 您可以使用 Amazon Simple Notification Service (SNS)，在每次因使用者 API 活動而建立、更新或修改受支援的 AWS 資源時傳送通知給您。
- 您可以使 EventBridge 用 Amazon 偵測 AWS Config 事件狀態的變更並做出回應。

主題


- 使用 Amazon SQS 監控 AWS 資源變更
- AWS Config 使用 Amazon 監控 EventBridge


## 使用 Amazon SQS 監控 AWS 資源變更

AWS Config 每次因使用者 API 活動而建立、更新或修改支援的 AWS 資源時，都會使用 Amazon 簡單通知服務 (SNS) 傳送通知給您。但是，您可能只關心特定資源的組態變更。例如，您可能認為知道有人修改安全群組的組態非常重要，但不需要知道 Amazon EC2 執行個體每一次的標籤變更。或者，您可能希望撰寫在特定資源更新時執行特定動作的程式。例如，您可能會希望在安全群組組態變更時啟動特定工作流程。如果您想要以程式設計方式使用這些或其他方式的資料，請使用 Amazon 簡單佇列服務佇列作為 Amazon SNS 的通知端點。 AWS Config

> **Note**
>
> 從 Amazon SNS 傳送通知的形式也可能為：電子郵件、傳送至啟用 SMS 的行動電話及智慧型手機的簡訊服務 (SMS) 訊息、傳送至行動裝置上應用程式的通知訊息，或是傳送至一或多個 HTTP 或 HTTPS 端點通知訊息。

您可以讓單一 SQS 佇列訂閱多個主題，無論每個區域都有一個主題，還是每個區域的每個帳戶都有一個主題。您必須讓佇列訂閱您所需的 SNS 主題。(您可以使多個佇列訂閱同一個 SNS 主題。) 如需詳細資訊，請參閱《將 Amazon SNS 訊息傳送至 Amazon SQS 佇列》。

## Amazon SQS 的許可

若要搭配使用 Amazon SQS AWS Config，您必須設定一項政策，以授予帳戶許可，才能執行 SQS 佇列上允許的所有動作。以下範例政策會授予編號為 111122223333 的帳戶和編號為 444455556666 的帳戶許可，將關於每個組態變更的訊息傳送至名為 arn:aws:sqs:us-east-2:444455556666:queue1 的佇列。

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

您也必須建立政策，授予 SNS 主題和訂閱該主題 SQS 佇列之間連線的許可。以下是範例政策，允許使用 Amazon 資源名稱 (ARN) 陣列的 SNS 主題:aw:ns: SNS: 美國東部-2:11112222333: 測試主題對名為 ARN 的佇列執行任何動作:aw:sq: test-topic-queue

> **Note**
>
> SNS 主題和 SQS 佇列的帳戶必須位於相同區域。

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

每個政策可包含僅涵蓋單一佇列 (而非多個佇列) 的陳述式。如需 Amazon SQS 政策其他限制的相關資訊，請參閱《Amazon SQS 政策的特殊資訊》。

## AWS Config 使用 Amazon 監控 EventBridge

Amazon EventBridge 提供近乎即時的系統事件串流，用於描述 AWS 資源變更。使 EventBridge 用 Amazon 偵測 AWS Config 事件狀態的變化並做出反應。

您可以建立規則，在有狀態轉換或有轉移到一或多個與您相關的狀態時執行。然後，當事件符合您在規則中指定的值時，Amazon 會根據您建立的規則 EventBridge 叫用一或多個目標動作。根據事件的類型，您可能會想要傳送通知、擷取事件資訊，採取修正動作、啟動事件，或採取其他動作。

但是，在建立事件規則之前 AWS Config，您應該執行下列動作：

- 熟悉中的事件、規則和目標。 EventBridge有關更多信息，請參閱什麼是 Amazon EventBridge？

- 如需如何開始使用 EventBridge 和設定規則的詳細資訊，請參閱 Amazon 入門 EventBridge。
- 建立您將在事件規則中使用的一或多個目標。

主題

- Amazon EventBridge 格式 AWS Config
- 創建 Amazon EventBridge 規則 AWS Config

## Amazon EventBridge 格式 AWS Config

的 EventBridge 事件 AWS Config 具有下列格式：

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

## 創建 Amazon EventBridge 規則 AWS Config

使用下列步驟建立在發出的事件上觸發的 EventBridge 規則。 AWS Config盡可能發出事件。

1. 在導覽窗格中，選擇規則。
2. 選擇建立規則。
3. 輸入規則的名稱和描述。

   在同一個區域和同一個事件匯流排上，規則不能與另一個規則同名。

4. 針對規則類型，選擇具有事件模式的規則。
5. 對於事件來源，請選擇AWS 事件或 EventBridge 合作夥伴事件。
6. (選用) 範例事件類型 請選擇 AWS 事件。
7. (選用) 範例事件 請選擇會觸發以下規則的事件類型：
   - 選擇「AWS API 呼叫方式」， CloudTrail以根據對此服務進行的 API 呼叫的規則為基礎。如需有關建立此類型規則的詳細資訊，請參閱教學課程：針對 AWS CloudTrail API 呼叫建立 Amazon EventBridge 規則。
   - 選擇 Config Configuration Item Change (設定組態項目變更) 以在您帳戶中的資源發生變更時取得通知。

     如這些支援文章所述，您可 EventBridge 以使用在建立或刪除資源時接收自訂電子郵件通知，如何在 AWS 帳戶 使用 AWS Config 服務中建立資源時接收自訂電子郵件通知？ 以及如何在 AWS 帳戶 使用 AWS Config 服務中刪除資源時接收自訂電子郵件通知？ 。
   - 選擇 Config Rules Compliance Change (設定規則合規性變更) 以在針對您規則進行的合規性檢查失敗時接收通知。

     如本支援文章所述，您可 EventBridge 以使用在資源不相容時接收自訂電子郵件通知。如何在 AWS 資源不相容時收到通知？ AWS Config。
   - 選擇 Config Rules Re-evaluation Status (設定規則重新評估狀態) 以取得重新評估狀態通知。
   - 選擇 Config Configuration Snapshot Delivery Status (設定組態快照交付狀態) 以取得組態快照交付狀態通知。
   - 選擇 Config Configuration History Delivery Status (設定組態歷史記錄交付狀態) 以取得組態歷史記錄交付狀態通知。
8. 建立方法 請選擇 使用模式表單。
9. 在事件來源欄位中，選擇 AWS 服務。
10. AWS 服務 請選擇 Config。
11. 事件類型 請選擇會觸發規則的事件類型：
   - 選擇「所有事件」以建立適用於所有 AWS 服務的規則。若您選擇此選項，您將無法選擇特定訊息類型、規則名稱、資源類型，或資源 ID。
   - 選擇「AWS API 呼叫方式」， CloudTrail以根據對此服務進行的 API 呼叫的規則為基礎。如需有關建立此類型規則的詳細資訊，請參閱教學課程：針對 AWS CloudTrail API 呼叫建立 Amazon EventBridge 規則。
   - 選擇 Config Configuration Item Change (設定組態項目變更) 以在您帳戶中的資源發生變更時取得通知。

如這些支援文章所述，您可 EventBridge 以使用在建立或刪除資源時接收自訂電子郵件通知，如何在 AWS 帳戶 使用 AWS Config 服務中建立資源時接收自訂電子郵件通知？ 以及如何在 AWS 帳戶 使用 AWS Config 服務中刪除資源時接收自訂電子郵件通知？ 。

- 選擇 Config Rules Compliance Change (設定規則合規性變更) 以在針對您規則進行的合規性檢查失敗時接收通知。

  如本支援文章所述，您可 EventBridge 以使用在資源不相容時接收自訂電子郵件通知。如何在 AWS 資源不相容時收到通知？ AWS Config。
- 選擇 Config Rules Re-evaluation Status (設定規則重新評估狀態) 以取得重新評估狀態通知。
- 選擇 Config Configuration Snapshot Delivery Status (設定組態快照交付狀態) 以取得組態快照交付狀態通知。
- 選擇 Config Configuration History Delivery Status (設定組態歷史記錄交付狀態) 以取得組態歷史記錄交付狀態通知。

12 選擇 Any message type (任何訊息類型) 以接收任何類型的通知。選擇 Specific message type(s) (特定訊息類型) 來接收下列通知類型：

- 如果您選擇 ConfigurationItemChangeNotification，則會在 AWS Config 評估的資源配置已變更時收到訊息。
- 如果您選擇 [ComplianceChange通知]，則會在 AWS Config 評估資源的符合性類型變更時收到訊息。
- 如果您選擇 ConfigRulesEvaluationStarted，則會在 AWS Config 開始針對指定資源評估規則時收到訊息。
- 如果您選擇 ConfigurationSnapshotDeliveryCompleted，則會在 AWS Config 成功將組態快照交付到 Amazon S3 儲存貯體時收到訊息。
- 如果您選擇 ConfigurationSnapshotDeliveryFailed，則會在 AWS Config 無法將組態快照交付到 Amazon S3 儲存貯體時收到訊息。
- 如果您選擇 ConfigurationSnapshotDeliveryStarted，則會在 AWS Config 開始將組態快照交付到 Amazon S3 儲存貯體時收到訊息。
- 如果您選擇 ConfigurationHistoryDeliveryCompleted，則會在 AWS Config 成功將組態歷史記錄交付到 Amazon S3 儲存貯體時收到訊息。

13 如果您從 [事件類型] 下拉式清單中選擇特定的事件類型，請選擇 [任何資源類型] 以建立適用於所有 AWS Config 支援資源類型的規則。

  或選擇 Specific resource type(s) (特定資源類型) 然後輸入 AWS Config 支援的資源類型 (例如，`AWS::EC2::Instance`)。

14. 如果您從 事件類型 下拉式清單中選擇特定的事件類型，請選擇 任何資源 ID 以包含所有 AWS Config 支援的資源 ID。

    或選擇 Specific resource ID(s) (特定資源 ID) 然後輸入 AWS Config 支援的資源 ID (例如，`i-04606de676e635647`)。
15. 如果您從 事件類型 下拉式清單中選擇特定的事件類型，請選擇 任何規則名稱 以包含所有 AWS Config 支援的規則。

    或選擇 Specific rule name(s) (特定規則名稱) 然後輸入 AWS Config 支援的規則 (例如 required-tags)。
16. 選取目標 請選擇您準備用於此規則的目標類型，再設定此類型需要的任何其他選項。
17. 顯示的欄位會隨您選擇的服務而異。請視需要輸入此目標類型的特定資訊。
18. 對於許多目標類型， EventBridge 需要將事件傳送至目標的權限。在這些情況下， EventBridge 可以建立執行規則所需的 IAM 角色。
    - 如需自動建立 IAM 角色，請選擇 為此特定資源建立新角色。
    - 若要使用您早前建立的 IAM 角色，請選擇 Use existing role (使用現有角色)。
19. (選用) 選擇 Add target (新增目標)，為此規則新增另一個目標。
20. (選用) 為規則輸入一或多個標籤。如需詳細資訊，請參閱 Amazon EventBridge 標籤。
21. 檢閱您的規則設定，確定其符合您的事件監控要求。
22. 選擇 建立 確認您選取的項目。

# AWS Config 搭配使用介面 Amazon VPC 端點

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 託管資 AWS 源，則可以在 VPC 和. 之間建立私有連接。 AWS Config您可以使用此連線從您的 VPC 與 AWS Config 進行通訊，而無需透過公有網際網路。

Amazon VPC 是一項 AWS 服務，可用於在您定義的虛擬網路中啟動 AWS 資源。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。介面 VPC 私人雲端端點的支援是一種使用具有私有 IP 位址的 elastic network interface AWS PrivateLink，在 AWS 服務之間進行私人通訊的 AWS 技術。若要將 VPC 連接到 AWS Config，您需要為的定義介面 VPC 端點。 AWS Config 這種類型的端點可讓您將 VPC 連線到 AWS 服務。端點提供可靠、可擴充的連線能力， AWS Config 無需網際網路閘道、網路位址轉譯 (NAT) 執行個體或 VPN 連線。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的什麼是 Amazon VPC。

下列步驟適用於 Amazon VPC 的使用者。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的入門。

## 為以下項目建立 VPC 端點 AWS Config

若要開 AWS Config 始使用您的 VPC，請為. AWS Config您不需要變更的設定 AWS Config。 AWS Config 使用其公有端點呼叫其他 AWS 服務。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的建立界面端點。

# 常見問答集

## 無法看到我最新的組態變更

### 我可以預期立即檢視我的組態變更嗎？

AWS Config 通常會在偵測到變更之後或您指定的頻率，立即記錄資源的組態變更。但是，這是在最大努力的基礎上，有時可能需要更長的時間。如果問題在一段時間後仍然存在，請聯絡AWS Support並提供 Amazon 支援的 AWS Config 指標 CloudWatch。如需這些測量結果的相關資訊，請參閱AWS Config 使用狀況和成功測

## 間接關係 AWS Config

主題


- 什麼是資源關係？
- 什麼是資源的直接和間接關係？
- 哪些間接關係 AWS Config 支持？
- 如何根據直接和間接關係建立組態項目？
- 由於間接關係而產生的組態項目有哪些？
- 如何擷取與間接關係相關的組態資料？


### 什麼是資源關係？

在中 AWS，資源是指可管理的實體，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、 AWS CloudFormation 堆疊或 Amazon S3 儲存貯體。 AWS Config 是一項服務，可在偵測到記錄的資源類型變更時或以您設定的錄製頻率建立組態項目 (CI) 來追蹤和監視資源。例如，當設定 AWS Config 為追蹤 Amazon EC2 執行個體時，它會在每次建立、更新或刪除執行個體時建立組態項目。由建立的每個組態項目都 AWS Config 有多個欄位`accountId`，包括 `arn` (Amazon 資源名稱) `awsRegion` `configuration`、`tags`、、和`relationships`。CI 的關係欄位可 AWS Config 以顯示資源如何相互連結。例如，某個關係可能表示 ID 為 `vol-123ab45d` 的 Amazon EBS 磁碟區已連接至 ID 為 `i-a1b2c3d4` 的 Amazon EC2 執行個體，該執行個體與安全群組 `sg-ef678hk` 相關聯。

## 什麼是資源的直接和間接關係？

AWS Config 從組態欄位 (稱為「直接」關係) 衍生大多數資源類型的關係。直接關係是資源 (A) 和另一個資源 (B) 之間的單向連接 (A→B)，通常從資源 (A) 的描述 API 回應中獲得。過去，對於一些 AWS Config 初始支援的資源類型，它也會從其他資源的組態擷取關係，建立雙向的「間接」關係 (B→A)。例如，因為安全群組包含在 Amazon EC2 執行個體的描述 API 回應中，所以 Amazon EC2 執行個體與其安全群組之間的關係為直接關係。另一方面，因為敘述一個安全群組不會傳回與其關聯之執行個體的任何相關資訊，所以安全群組與 Amazon EC2 執行個體之間的關係為間接關係。因此，當偵測到資源組態變更時， AWS Config 不僅會為該資源建立 CI，還會為任何相關資源 (包括具有間接關係的資源) 產生 CI。例如，當 AWS Config 偵測到 Amazon EC2 執行個體中的變更時，會為執行個體建立 CI，並為與執行個體關聯的安全群組建立 CI。

## 哪些間接關係 AWS Config 支持？

中支援下列間接資源關係 AWS Config。

| 資源類型 | 與資源類型間接相關 | | |
| --- | --- | --- | --- |
| AWS::EC2::RouteTable | AWS::EC2::Instance，AWS::EC2::NetworkInterface，AWS::EC2::Subnet，AWS::EC2::VPNGateway，AWS::EC2::VPC | | |
| AWS::EC2::EIP | AWS::EC2::Instance，AWS::EC2::NetworkInterface | | |
| AWS::EC2::Instance | AWS::EC2::SecurityGroup，AWS::EC2: | | |

| 資源類型 | 與資源類型間接相關 | | |
|---|---|---|---|
| | :Subnet ，AWS::EC2::VPC | | |
| AWS::EC2::NetworkInterface | AWS::EC2::SecurityGroup ，AWS::EC2::Subnet ，AWS::EC2::VPC | | |
| AWS::EC2::NetworkACL | AWS::EC2::Subnet ，AWS::EC2::VPC | | |
| AWS::EC2::VPNConnection | AWS::EC2::VPNGateway ，AWS::EC2::CustomerGateway | | |
| AWS::EC2::InternetGateway | AWS::EC2::VPC | | |
| AWS::EC2::SecurityGroup | AWS::EC2::VPC | | |
| AWS::EC2::Subnet | AWS::EC2::VPC | | |
| AWS::EC2::VPNGateway | AWS::EC2::VPC | | |

## 如何根據直接和間接關係建立組態項目？

針對資源之間的直接關係 (A→B)，對資源 B 的任何組態變更，也會啟動資源 A 的組態項目 (CI)。同樣地，針對間接關係 (B→A)，當資源 A 的組態變更時，資源 B 會產生新的 CI。例如，Amazon EC2 執行

個體與安全群組為直接關係，因此對安全群組的任何組態變更，都會為安全群組產生 CI，並為 EC2 執行個體產生 CI。同樣地，Amazon EC2 執行個體與其安全群組為間接關係，因此對 EC2 執行個體進行的任何組態變更，都會為 Amazon EC2 執行個體產生 CI，並為安全群組產生 CI。

## 由於間接關係而產生的組態項目有哪些？

下列是由於間接資源關係而產生的其他組態項目 (CI)。

| 會針對下列資源類型變更組態： | 會針對下列資源類型產生 CI： | | |
| --- | --- | --- | --- |
| AWS::EC2::RouteTable | AWS::EC2::Instance ，AWS::EC2::NetworkInterface ，AWS::EC2::Subnet ，AWS::EC2::VPNGateway ，和 AWS::EC2::VPC | | |
| AWS::EC2::EIP | AWS::EC2::Instance ，AWS::EC2::NetworkInterface | | |
| AWS::EC2::Instance | AWS::EC2::SecurityGroup ，AWS::EC2::Subnet ，AWS::EC2::VPC | | |
| AWS::EC2::NetworkInterface | AWS::EC2::SecurityGroup ，AWS::EC2: | | |

| 會針對下列資源類型變更組態： | 會針對下列資源類型產生 CI： | | |
|---|---|---|---|
| | :Subnet ，AWS::EC2::VPC | | |
| AWS::EC2::NetworkACL | AWS::EC2::Subnet ，AWS::EC2::VPC | | |
| AWS::EC2::VPNConnection | AWS::EC2::VPNGateway ，AWS::EC2::Customer Gateway | | |
| AWS::EC2::Internet Gateway | AWS::EC2::VPC | | |
| AWS::EC2::SecurityGroup | AWS::EC2::VPC | | |
| AWS::EC2::Subnet | AWS::EC2::VPC | | |
| AWS::EC2::VPNGateway | AWS::EC2::VPC | | |

## 如何擷取與間接關係相關的組態資料？

您可以在 AWS Config 進階查詢中執行結構化查詢語言 (SQL) 查詢，以擷取與間接資源關係相關的組態資料。例如，如果您想要擷取與安全群組相關的 Amazon EC2 執行個體清單，請使用下列查詢：

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
```

```
    AND
    relationships.resourceId = 'sg-234213'
```

# AWS Config 使用 AWS SDK 的程式碼範例

下列程式碼範例顯示如何搭 AWS Config 配 AWS 軟體開發套件 (SDK) 使用。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境和跨服務範例中查看內容中的動作。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

程式碼範例

- AWS Config 使用 AWS SDK 的動作
  - 搭DeleteConfigRule配 AWS 開發套件或 CLI 使用
  - 搭DescribeComplianceByConfigRule配 AWS 開發套件或 CLI 使用
  - 搭DescribeComplianceByResource配 AWS 開發套件或 CLI 使用
  - 搭DescribeConfigRuleEvaluationStatus配 AWS 開發套件或 CLI 使用
  - 搭DescribeConfigRules配 AWS 開發套件或 CLI 使用
  - 搭DescribeConfigurationRecorderStatus配 AWS 開發套件或 CLI 使用
  - 搭DescribeConfigurationRecorders配 AWS 開發套件或 CLI 使用
  - 搭DescribeDeliveryChannels配 AWS 開發套件或 CLI 使用
  - 搭GetComplianceDetailsByConfigRule配 AWS 開發套件或 CLI 使用
  - 搭GetComplianceDetailsByResource配 AWS 開發套件或 CLI 使用
  - 搭GetComplianceSummaryByConfigRule配 AWS 開發套件或 CLI 使用
  - 搭GetComplianceSummaryByResourceType配 AWS 開發套件或 CLI 使用
  - 搭PutConfigRule配 AWS 開發套件或 CLI 使用
  - 搭PutDeliveryChannel配 AWS 開發套件或 CLI 使用

## AWS Config 使用 AWS SDK 的動作

下列程式碼範例示範如何使用 AWS SDK 執 AWS Config 行個別動作。這些摘錄會呼叫 AWS Config API，是來自必須在內容中執行的大型程式碼摘錄。每個範例都包含一個連結 GitHub，您可以在其中找到設定和執行程式碼的指示。

下列範例僅包含最常使用的動作。如需完整清單，請參閱《AWS Config API 參考》。

範例

- 搭DeleteConfigRule配 AWS 開發套件或 CLI 使用
- 搭DescribeComplianceByConfigRule配 AWS 開發套件或 CLI 使用
- 搭DescribeComplianceByResource配 AWS 開發套件或 CLI 使用
- 搭DescribeConfigRuleEvaluationStatus配 AWS 開發套件或 CLI 使用
- 搭DescribeConfigRules配 AWS 開發套件或 CLI 使用
- 搭DescribeConfigurationRecorderStatus配 AWS 開發套件或 CLI 使用
- 搭DescribeConfigurationRecorders配 AWS 開發套件或 CLI 使用
- 搭DescribeDeliveryChannels配 AWS 開發套件或 CLI 使用
- 搭GetComplianceDetailsByConfigRule配 AWS 開發套件或 CLI 使用
- 搭GetComplianceDetailsByResource配 AWS 開發套件或 CLI 使用
- 搭GetComplianceSummaryByConfigRule配 AWS 開發套件或 CLI 使用
- 搭GetComplianceSummaryByResourceType配 AWS 開發套件或 CLI 使用
- 搭PutConfigRule配 AWS 開發套件或 CLI 使用
- 搭PutDeliveryChannel配 AWS 開發套件或 CLI 使用

## 搭`DeleteConfigRule`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`DeleteConfigRule`。

CLI

AWS CLI

刪除 AWS 組 Config 規則

下列命令會刪除名為的 AWS Config 規則`MyConfigRule`：

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DeleteConfigRule中的。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DeleteConfigRule中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`DescribeComplianceByConfigRule`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`DescribeComplianceByConfigRule`。

CLI

AWS CLI

取得 AWS Config 規則的合規性資訊

下列命令會針對一或多個資源違反的每個 AWS Config 規則傳回符合性 AWS 資訊：

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

在輸出中，每個`CappedCount`屬性的值表示有多少資源不符合相關規則。例如，下列輸出表示 3 個資源不符合名為的規則`InstanceTypesAreT2micro`。

輸出：

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
```

```
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeComplianceByConfigRule中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例擷取規則的相容性明細 ebs-optimized-instance，而規則沒有目前的評估結果，因此會傳回 UNADICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

輸出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

範例 2：此範例會傳回規則的不相容資源數目。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

輸出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeComplianceByConfigRule式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

# 搭DescribeComplianceByResource配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用DescribeComplianceByResource。

CLI

AWS CLI

取得資源的法規遵循 AWS 資訊

下列命令會針對 AWS Config 記錄且違反一或多個規則的每個 EC2 執行個體傳回合規資訊：

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

在輸出中，每個CappedCount屬性的值指示資源違反了多少規則。例如，下列輸出表示執行個體i-1a2b3c4d違反了 2 個規則。

輸出：

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
```

```
            }
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeComplianceByResource中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會檢查**AWS::SSM::ManagedInstanceInventory**資源類型是否符合「相容」相容性類型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

輸出：

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeComplianceByResource式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭**DescribeConfigRuleEvaluationStatus**配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用DescribeConfigRuleEvaluationStatus。

## CLI

### AWS CLI

取得組態規則的狀 Con AWS fig 資訊

下列命令會傳回名為之 AWS Config 規則的狀態資訊`MyConfigRule`：

```
aws configservice describe-config-rule-evaluation-status --config-rule-names
 MyConfigRule
```

輸出：

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeConfigRuleEvaluationStatus中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例會傳回指定組態規則的狀態資訊。

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

輸出：

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
```

```
ConfigRuleId                  : config-rule-kvq1wk
ConfigRuleName                : root-account-mfa-enabled
FirstActivatedTime            : 8/27/2019 8:05:17 AM
FirstEvaluationStarted        : True
LastErrorCode                 :
LastErrorMessage              :
LastFailedEvaluationTime      : 1/1/0001 12:00:00 AM
LastFailedInvocationTime      : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                 : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                  : config-rule-z1s23b
ConfigRuleName                : vpc-flow-logs-enabled
FirstActivatedTime            : 8/14/2019 6:23:44 AM
FirstEvaluationStarted        : True
LastErrorCode                 :
LastErrorMessage              :
LastFailedEvaluationTime      : 1/1/0001 12:00:00 AM
LastFailedInvocationTime      : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeConfigRuleEvaluationStatus式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`DescribeConfigRules`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`DescribeConfigRules`。

CLI

AWS CLI

若要取得 AWS Config 規則的詳細資訊

下列命令會傳回名為之 AWS Config 規則的詳細資料`InstanceTypesAreT2micro`：

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

輸出：

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeConfigRules中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例會列出帳戶的組態規則，以及選取的屬性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

輸出：

```
ConfigRuleName                                   ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                   ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                            config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                              config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required       config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeConfigRules式參考中的。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class ConfigWrapper:
```

```
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DescribeConfigRules中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`DescribeConfigurationRecorderStatus`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`DescribeConfigurationRecorderStatus`。

## CLI

### AWS CLI

取得組態錄製程式的狀態資訊

下列命令會傳回預設組態記錄程式的狀態：

```
aws configservice describe-configuration-recorder-status
```

輸出：

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeConfigurationRecorderStatus中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例會傳回組態記錄器的狀態。

```
Get-CFGConfigurationRecorderStatus
```

輸出：

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
```

```
LastStopTime          : 10/11/2019 10:13:46 AM
Name                  : default
Recording             : True
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeConfigurationRecorderStatus式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`DescribeConfigurationRecorders`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`DescribeConfigurationRecorders`。

CLI

AWS CLI

取得有關組態記錄程式的詳細資料

下列命令會傳回有關預設組態記錄程式的詳細資料：

```
aws configservice describe-configuration-recorders
```

輸出：

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeConfigurationRecorders中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會傳回組態記錄器的詳細資訊。

```
Get-CFGConfigurationRecorder | Format-List
```

輸出：

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeConfigurationRecorders式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`DescribeDeliveryChannels`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`DescribeDeliveryChannels`。

CLI

AWS CLI

取得有關傳送管道的詳細資訊

下列命令會傳回有關傳送通道的詳細資料：

```
aws configservice describe-delivery-channels
```

輸出：

```
{
    "DeliveryChannels": [
        {
```

```
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeDeliveryChannels中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會擷取區域的傳送管道並顯示詳細資訊。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

輸出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程DescribeDeliveryChannels式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`GetComplianceDetailsByConfigRule`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`GetComplianceDetailsByConfigRule`。

CLI

AWS CLI

若要取得 Con AWS fig 規則的評估結果

下列命令會針對所有不符合名為的 AWS Config 規則的資源傳回評估結果`InstanceTypesAreT2micro`：

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

輸出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
```

```
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceDetailsByConfigRule中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例取得規則的評估結果， access-keys-rotated 並傳回依規定型態分組的輸出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

輸出：

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

範例 2：此範例會查詢相容資源規則 access-keys-rotated 的符合性詳細資料。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

輸出：

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
```

```
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceDetailsByConfigRule式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`GetComplianceDetailsByResource`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`GetComplianceDetailsByResource`。

CLI

AWS CLI

若要取得 AWS 資源的評估結果

下列命令會針對 EC2 執行個體`i-1a2b3c4d`不符合的每個規則傳回評估結果：

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

輸出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceDetailsByResource中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：指定資源的此範例迴避結果。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

輸出：

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceDetailsByResource式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

# 搭GetComplianceSummaryByConfigRule配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用GetComplianceSummaryByConfigRule。

## CLI

### AWS CLI

取得 Con AWS fig 規則的合規摘要

下列命令會傳回符合規則的數目以及不相容的數目：

```
aws configservice get-compliance-summary-by-config-rule
```

在輸出中，每個CappedCount屬性的值表示有多少規則相容或不相容。

輸出：

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceSummaryByConfigRule中的。

## PowerShell

### 適用的工具 PowerShell

範例 1：此範例會傳回不相容的 Config 規則數目。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

輸出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceSummaryByConfigRule式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭GetComplianceSummaryByResourceType配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用GetComplianceSummaryByResourceType。

CLI

AWS CLI

取得所有資源類型的符合性摘要

下列命令會傳回不相容的 AWS 資源數目以及相容的編號：

```
aws configservice get-compliance-summary-by-resource-type
```

在輸出中，每個CappedCount屬性的值表示有多少資源相容或不相容。

輸出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
```

```
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

取得特定資源類型的符合性摘要

下列命令會傳回不相容的 EC2 執行個體數目以及符合規定的數目：

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

在輸出中，每個CappedCount屬性的值表示有多少資源相容或不相容。

輸出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考GetComplianceSummaryByResourceType中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會傳回相容或不相容的資源數量，並將輸出轉換為 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程GetComplianceSummaryByResourceType式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`PutConfigRule`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`PutConfigRule`。

CLI

AWS CLI

若要新增 AWS 受管理的 Config 規則

以下命令提供 JSON 代碼來添加 AWS 託管 Config 規則：

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`是包含規則組態的 JSON 檔案：

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

對於`ComplianceResourceTypes`屬性，此 JSON 代碼將範圍限制為該`AWS::EC2::Instance`類型的資源，因此 AWS Config 將僅評估 EC2 實例違反規則。由於規則是受管理規則，因此`Owner`屬性會設定為`AWS`，且`SourceIdentifier`屬性會設定為規則識別元`REQUIRED_TAGS`。對於`InputParameters`屬性，會指定規則所需的標籤鍵`Owner`，`CostCenter`和。

如果命令成功， AWS Config 不會返回任何輸出。若要驗證規則組態，請執行 describe-config-rules 命令，然後指定規則名稱。

新增客戶管理的 Config 規則

下列命令提供 JSON 程式碼，以新增客戶管理的 Config 規則：

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`是包含規則組態的 JSON 檔案：

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
```

```
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

對於`ComplianceResourceTypes`屬性，此 JSON 代碼將範圍限制為該`AWS::EC2::Instance`類型的資源，因此 AWS Config 將僅評估 EC2 實例違反規則。由於此規則是客戶管理規則，因此`Owner`屬性會設定為`CUSTOM_LAMBDA`，並將`SourceIdentifier`屬性設定為 AWS Lambda 函數的 ARN。該`SourceDetails`對象是必需的。當 AWS Config 叫用 AWS Lambda 函數以根據規則評估資源時，針對`InputParameters`屬性指定的參數會傳遞至 Lambda 函數。

如果命令成功， AWS Config 不會返回任何輸出。若要驗證規則組態，請執行 describe-config-rules 命令，然後指定規則名稱。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考PutConfigRule中的。

## Python

### 適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class ConfigWrapper:
    """
```

```
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件PutConfigRule中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭`PutDeliveryChannel`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`PutDeliveryChannel`。

CLI

AWS CLI

若要建立傳送管道

下列命令會以 JSON 程式碼的形式提供傳遞通道的設定：

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

`deliveryChannel.json`檔案會指定傳送通道屬性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

此範例會設定下列屬性：

`name`-傳送管道的名稱。根據預設， AWS Config 會將名稱`default`指派給新的傳送通道。您無法使用指令更新傳送通道名稱。`put-delivery-channel`如需變更名稱的步驟，請參閱重新命名傳遞管道。 `s3BucketName`-Con AWS fig 交付組態快照和組態歷史記錄檔案的 Amazon S3 儲存貯體的名稱。如果您指定屬於另一個 AWS 帳戶的儲存貯體，則該儲存貯體必須具有授與 Config 存取權限的政策。 AWS 如需詳細資訊，請參閱《Amazon S3 儲存貯體許可》。

`snsTopicARN`-Amazon Amazon SNS 主題的 Amazon 資源名稱 (ARN)，組態會向其傳送有關組態變更的通知。如果您從其他帳戶選擇主題，則該主題必須具有授與 AWS Config 存取權限的政策。 AWS 如需詳細資訊，請參閱 Amazon SNS 主題的許可。

`configSnapshotDeliveryProperties`-包含`deliveryFrequency`屬性，可設定 AWS Config 傳遞組態快照的頻率，以及呼叫週期性組 Config 規則評估的頻率。

如果命令成功， AWS Config 不會返回任何輸出。若要驗證傳遞通道的設定，請執行 describe-delivery-channels 命令。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考PutDeliveryChannel中的。

PowerShell

適用的工具 PowerShell

範例 1：此範例會變更現有傳送管道的傳送頻率屬性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- 如需 API 詳細資訊，請參閱AWS Tools for PowerShell 指令程PutDeliveryChannel式參考中的。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭 AWS Config 配 AWS SDK 使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

# 文件歷史記錄

下表說明的文件的重要變更 AWS Config。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

- API 版本：2014 年 11 月 12 日
- 最新文件更新：2024 年 6 月 17 日

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 安全 IAM 更新 | 政`AWSConfigServiceRolePolicy` 策和`AWS_ConfigRole` 政策現在為 Amazon Elastic File System (Amazon EFS)、Amazon Redshift 和 適用於 SAP 的 AWS Systems Manager. 如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2024年6月17日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• 雲路-s3 桶公共訪問禁止<br>• 雲通道 S3-桶訪問日誌 | 2024年5月8日 |
| AWS Config 更新受管規則 | 在此版本中， AWS Config 支援下列受管規則：啟用 i am 外部存取分析器 | 2024年5月2日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• 啟用安全防護惡意軟體保護<br>• 啟用防護-rds 保護<br>• 安全防護-S3-保護啟用<br>• 檢查員-羔羊標準掃描啟用 | 2024年4月26日 |

| | | |
|---|---|---|
| AWS Config 使用 Amazon 簡化使用分析 CloudWatch | 在此版本中，用於監控 AWS Config 資料使用 CloudWatch 量的 Amazon 指標將僅顯示可計費用量。這意味著不可計費的用量將不再顯示在發送到的 Amazon CloudWatch 指標 AWS Config 和主控台中。 AWS Config 這可讓您使用 Amazon CloudWatch 指標驗證 AWS Config 設定和使用量，並將可計費用量與相關成本建立關聯。如需詳細資訊，請參閱AWS Config 使用狀況和成功量度。 | 2024年4月26日 |
| AWS Config 更新受管規則 | 在此版本中， AWS Config 支援下列受管規則：i am-伺服器-憑證過期-檢查 | 2024年4月23 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• VPC-NG 端口限制檢查<br>• 雲跟踪全寫 S3 數據事件檢查<br>• 雲徑-全讀-S3-數據事件檢查 | 2024年4月17日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• 警衛-EK-保護審計啟用<br>• 防護-EK 保護-運行時啟用<br>• 啟用了防守羔羊保護<br>• 檢查器-ec2-掃描啟用<br>• 檢查器 ECR-掃描啟用<br>• 檢查器羔羊代碼掃描啟用<br>• 未受限制的無限制連接埠存取 | 2024年4月16日 |
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：ef s-掛載目標可公開存取/存取 | 2024年3月20日 |
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• DMS-海王星 IAM 授權啟用<br>• 啟用 DMS-蒙古 DB-身份驗證<br>• 啟用 DMS-雷迪斯<br>• Dax-tls 端點加密<br>• eks-群集秘密加密<br>• 中國火花交付流加密<br>• mq-雲觀察審計日誌啟用<br>• mq-雲觀察審計日誌啟用<br>• 打開搜索主要節點容錯<br>• 命形器-端點配置-配置-實例計數<br>• 與組織內共用的服務目錄<br>• 傳輸家庭服務器-無 FTP | 2024年2月26日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在為 Prometheus、Amazon、Amazon Cognito、Amazon、Amazon FSX、AWS Identity and Access Management (IAM) CloudWatch、、、Amazon Redshift 無伺服器 ElastiCache、Amazon 和亞馬遜簡單通知服務 (Amazon SNS) 授予其他亞馬遜 SageMaker託管服務的許可。 AWS Glue AWS Lambda AWS RAM如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2024年2月22 日 |
| AWS Config 更新受管規則 | 在此版本中， AWS Config 支援下列受管規則：已啟用 S3 儲存貯體跨區域複寫 | 2024年2月12日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新 AWS AppConfig的 Amazon CloudWatch 顯而易見的 AWS Identity and Access Management (IAM)、Amazon 記憶數據庫 (MemoryDB)、Amazon 卡夫卡 (Amazon MSK)、亞馬遜 Redshift 和資源類型的亞馬遜受管串流。 AWS Transfer Family 如需詳細資訊，請參閱《支援的資源類型》。 | 2024年2月6日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此版本中， AWS Config 支援下列受管規則：Mac ie-自動敏感資料探索檢查 | 2024年1月29日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新的 Amazon AppStream、 AWS Key Management Service (AWS KMS)、Amazon Relationa l Database Service 服務 (Amazon RDS)、Amazon 認知、亞馬遜彈性運算雲端 (Amazon EC2)、EC2 Image Builder、、、亞馬遜 AWS Ground Station AWS Mainframe Modernization QuickSight、亞馬 Amazon Redshift 和 AWS Systems Manager 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2024 年 1 月 3 日 |
| 每個帳戶每個區域的 AWS Config 規則數量上限會增加服務限制 | 在此版本中，每個帳戶 AWS Config 支援每個 AWS 區域 1000 個 AWS Config 規則。此增加適用於所有已部署規則的總數，包括 AWS Config 受管規則、 AWS Config 自訂規則、一 AWS Config 致性套件、 AWS Security Hub 控制項、 AWS Firewall Manager 政策和每個帳戶每個區域的 AWS Backup 備份計劃。如需詳細資訊，請參閱 服務限制。 | 2023 年 12 月 19 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• s3-meets-restore-time-target<br>• ebs-meets-restore-time-target<br>• ec2-meets-restore-time-target<br>• rds-meets-restore-time-target<br>• efs-meets-restore-time-target<br>• fsx-meets-restore-time-target<br>• aurora-meets-restore-time-target<br>• dynamodb-meets-restore-time-target | 2023 年 12 月 19 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策現在授予其他許可 AWS AppConfig，適用於 Prometheus，（ ），AWS Database Migration Service （AWS DMSAWS Identity and Access Management）IAM，Amazon 卡夫卡（Amazon MSK），Amazon CloudWatch 日誌和 Amazon 簡單存儲服務（Amazon S3）的亞馬遜託管服務。 AWS Organizations如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 12 月 5 日 |
| 預覽版本：用於進階查詢的自然語言查詢處理器 | 在此版本中，您可以使用自然語言查詢處理器進行進階查詢，該處理器使用生成人工智慧 (生成 AI) 功能，讓您以簡單的英文提出問題並將其轉換為 ready-to-use 查詢格式。使用自然語言查詢處理器，您可以查詢您的 AWS 帳戶 或整個 AWS 組織。如需詳細資訊，請參閱進階查詢的自然語言查詢處理器。 | 2023 年 11 月 26 日 |

| | | |
|---|---|---|
| 定期記錄 | 在此版本中， AWS Config 支援定期記錄。定期記錄可讓您擷取固定期間內資源的最新組態變更。現在，您可以將組態記錄器的預設頻率設定為「每日」，讓您接收代表過去 24 小時期間內資源最新狀態的組態項目 (CI)，前提是該項目必須與先前的 CI 記錄不同。 AWS Config 主控台也引進了全新的錄製策略體驗，您也可以在其中覆寫特定資源類型的錄製頻率，或從錄製中排除特定資源類型。這有助於使您的設定符合您的細微需求。<br><br>新增了下列資料類型：<br><br>• RecordingMode<br>• RecordingMode覆寫<br><br>更新了下列資料類型：<br><br>• PutConfiguration錄音機<br>• ConfigurationRecorder<br>• BaseConfiguration項目<br>• ConfigurationItem<br><br>更新了《開發人員指南》中的下列頁面：<br><br>• 重新編碼資源 AWS<br>• 使用 AWS Config 主控台 AWS Config 進行設定 \| 一鍵式設定 | 2023 年 11 月 26 日 |

- 使用 AWS Config 主控 AWS Config 台設定 | 手動設定
- 使用 AWS CLI AWS Config 進行設定

| | | |
|---|---|---|
| 安全 IAM 更新 | 該AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策現在授予 Amazon Cognito，Amazon Connect，Amazon EMR AWS Ground Station，Amazon MemoryDB AWS Mainframe Modernization，Amazon， AWS Organizations亞馬 Amazon Relational Database Service（Amazon RDS）QuickSight，Amazon Redshift，Amazon 路線 53 和。 AWS Service Catalog AWS Transfer Family<br><br>AWSConfigServiceRolePolicy 政策和 AWS_ConfigRole 政策現在也會新增 AWSConfigServiceRolePolicyStatementID 、AWSConfigSLRLogStatementID 、AWSConfigSLRLogEventStatementID 、AWSConfigSLRApiGatewayStatementID 和 AWSConfigServiceRolePolicy 政策的安全性識別碼 (SID)。<br><br>如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 11 月 17 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• acm-pca-root-ca-disabled<br>• dynamodb-table-deletion-protection-enabled<br>• ec2-client-vpn-connection-log-enabled<br>• eks-cluster-log-enabled<br>• emr-block-public-access<br>• fsx-windows-audit-log-configured<br>• fsx-openzfs-copy-tags-enabled<br>• fsx-lustre-copy-tags-to-backups<br>• msk-enhanced-monitoring-enabled<br>• mq-auto-minor-version-upgrade-enabled<br>• neptune-cluster-multi-az-enabled<br>• opensearch-update-check<br>• s3-access-point-in-vpc-only<br>• s3-access-point-public-access-blocks<br>• s3-bucket-mfa-delete-enabled | 2023 年 11 月 9 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使用將組態變更記錄 AWS Config 到新的 AWS Identity and Access Management (IAM) AWS Network Manager、AWS Private Certificate Authority (AWS Private CA)、AWS App Mesh、Amazon Connect、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Container Service (Amazon ECS)、 AWS IoT AWS IoT TwinMaker、Amazon Managed Streaming for Apache Kafka Connect (Amazon MSK Connect) 和資源類型。 AWS Lambda AWS 資源總管 如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 11 月 3 日 |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 更新下列一致性套件：BNM RMit 的營運最佳實務 | 2023 年 10 月 26 日 |

| | | |
|---|---|---|
| 彙總工具的合規和清查儀表板 | 在此版本中， AWS Config 將合規儀表板頁面和庫存儀表板頁面新增至 AWS Config 主控台中的彙總檢視。<br><br>對於合規儀表板頁面，您可以檢視自動化儀表板，其中包含小工具，摘要了有關您彙總工具內資源合規的洞察，例如依不合規資源排序的前 10 個資源類型、依不合規規則排序的前 10 個帳戶層級一致性套件等。<br><br>對於清查儀表板頁面，您可以檢視自動化儀表板，其中包含小工具，摘要了有關您彙總工具內資源組態資料的洞察，例如依資源計數排序的前 10 個資源類型、依資源計數排序的前 10 個帳戶等。<br><br>如需圖形和圖表的資訊，請參閱《合規儀表板》和《清查儀表板》。 | 2023 年 10 月 23 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在授予額外的許可 AWS Private CA AWS App Mesh,, Amazon Connect, Amazon CloudWatch Elastic Container Service (Amazon ECS), Amazon 託管 Grafana, Amazon, Amazon 檢查器 GuardDuty, AWS IoT AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK),,,, 和 Amazon. AWS Lambda AWS Network Manager AWS Organizations SageMaker 如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 10 月 4 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新的 AWS IoT、、AWS IoT TwinMaker、、AWS IoT Wireless、Amazon Personalize 類型的 Apache 卡夫卡 (Amazon MSK)、Amazon、Amazon 和 Amazon SageMaker Inspector 資源類型的亞馬遜 AppStream受管串流。 AWS CodeBuild如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 10 月 4 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• docdb-cluster-deletion-protection-enabled<br>• docdb-cluster-audit-logging-enabled<br>• docdb-cluster-snapshot-public-prohibited<br>• mq-active-deployment-mode<br>• mq-rabbit-deployment-mode<br>• dms-auto-minor-version-upgrade-check<br>• dms-replication-task-target db-logging<br>• dms-replication-task-source db-logging<br>• dms-endpoint-ssl-configured<br>• custom-eventbus-policy-attached<br>• global-endpoint-event-replication-enabled<br>• route53-query-logging-enabled<br>• rds-aurora-mysql-audit-logging-enabled<br>• rds-cluster-auto-minor-version-upgrade-enable<br>• appsync-authorization-check<br>• netfw-deletion-protection-enabled<br>• wafv2-rulegroup-logging-enabled | 2023 年 9 月 21 日 |

| | | |
|---|---|---|
| | • msk-in-cluster-node-require-tls | |
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新下列一致性套件：<br>• Amazon S3 的操作最佳實務<br>• EC2 的操作最佳實務 | 2023 年 9 月 8 日 |
| 安全 IAM 更新 | 此原`AWSConfigServiceRolePolicy` 則現在會移除 AWS Systems Manager (Systems Manager) 的權限。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 9 月 6 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新的 Amazon CodeGuru 效能分析工具、、 AWS Elemental MediaConnect、AWS Transfer Family、Prometheus、、 AWS Batch和資源類型的 Amazon 受管服務。 AWS Cloud Map Amazon Route 53 Resolver 如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 9 月 6 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• athena-workgroup-encrypted-at-rest<br>• neptune-cluster-iam-database-authentication<br>• neptune-cluster-copy-tags-to-snapshot-enabled<br>• neptune-cluster-cloudwatch-log-export-enabled<br>• neptune-cluster-deletion-protection-enabled<br>• neptune-cluster-snapshot-encrypted<br>• neptune-cluster-backup-retention-check<br>• neptune-cluster-encrypted<br>• neptune-cluster-snapshot-public-prohibited<br>• docdb-cluster-backup-retention-check<br>• docdb-cluster-encrypted<br>• rds-cluster-encrypted-at-rest | 2023 年 8 月 10 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 通過此版本，您可以使用 AWS Config 將配置更改記錄到新的 AWS Amplify AppIntegrations，Amazon AWS App Mesh，Amazon Athena，Amazon 彈性計算雲（Amazon EC2），Amazon CloudWatch 顯然，Amazon Forecast，，AWS IoT Greengrass Version 2 AWS Ground Station AWS Elemental MediaConvert AWS Elemental MediaTailor，Amazon Managed Streaming for Apache Kafka（亞馬遜 MSK），Amazon Personalize 化，Amazon Pinpoint 和資源類型。 AWS Resilience Hub 如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 8 月 3 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策現在為 Amazon AppStream 2.0, Amazon, Amazon Connect AWS App Mesh, Amazon, AWS Identity and Access Management (IAM) AWS CloudFormation CloudFront AWS CodeArtifact, Amazon 檢查器 AWS CodeBuild,, AWS Glue GuardDuty, Amazon Managed Streaming for Apache Kafka 授予額外的許可 AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon 2.0, Amazon,, 亞馬遜路線 53 AWS Elemental MediaConnect AWS Network Manager AWS Organizations AWS 資源總管, 亞馬遜 Simple Storage Service (Amazon S3), 亞馬遜簡單通知服務 (Amazon SNS) 和 Amazon EC2 系統管理員 (SSM)。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 7 月 28 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新的 Amazon Kinesis、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon 針點、Amazon Simple Storage Service (Amazon S3)、Amazon Virtual Private Cloud (亞馬遜 VPC)、Amazon Kendra、Amazon Connect、、、 AWS CloudFormation AWS AppConfig AWS App Mesh AWS App Runner、和 AWS Database Migration Service (AWS DMS) 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 7 月 10 日 |
| 提高組織一致性套件的服務限制 | 在此版本中，在所有一致性套件中，每個區域的每個帳戶 AWS Config 支援 350 個 AWS Config 規則，以及每個組織 350 個組織 AWS Config 規則。如需詳細資訊，請參閱 服務限制。 | 2023 年 6 月 13 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | 該AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策現在為 Amazon 連接 AWS Amplify,, Amazon 託管服務 Prometheus AWS App Mesh, Amazon 雅典娜,,,, Amazon DynamoDB, Amazon DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch 明顯, Amazon Forecast,,,, (IAM), Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management (亞馬遜 MSK), Amazon Lightsail，亞馬遜日誌 AWS Organizations AWS IoT Greengrass AWS Ground Station CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor，Amazon Pinpoint，Amazon Virtual Private Cloud（Amazon VPC），Amazon Personalize 化，Amazon，Amazon QuickSight AWS Migration Hub Refactor Spaces，Amazon 簡單存儲服務（亞馬遜 S3） SageMaker，亞馬遜和. AWS Transfer Family如需詳細 | 2023 年 6 月 13 日 |

| | | |
|---|---|---|
| | 資訊，請參閱 AWS Config的 AWS 受管政策。 | |
| AWS Config 依資源類型的記錄排除 | 透過此版本，您 AWS Config 可以將特定類型的 AWS 資源從庫存追蹤和合規監控中排除，同時仍追蹤目前可用的所有其他支援資源類型 AWS Config，包括 future 將新增的資源類型。您可以使用此功能，專注於受到合規與控管標準約束的重要資源。<br><br>設定記錄程式和錄製檔群組的 API 更新向後相容，這表示它們可以與先前版本的 R PutConfigurationecorder API 搭配使用。您可以繼續使用與先前完全相同的方式來管理要記錄的資源類型，而不需要使用已更新或新的 API。<br><br>新增了下列資料類型：<br><br>• RecordingStrategy<br>• ExclusionByResourceTypes<br><br>更新了下列資料類型：<br><br>• PutConfiguration錄音機<br>• ConfigurationRecorder<br>• RecordingGroup<br><br>更新了《開發人員指南》中的下列頁面：<br><br>• 選取要記錄的資源 | 2023 年 6 月 9 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 通過此版本，您可以使用將配置更改記錄 AWS Config 到新的 Amazon Elastic Container Service (Amazon ECS)，Amazon Keyspaces（用於 Apache Cassandra），Amazon 彈性運算雲（Amazon EC2），Amazon CloudWatch 明顯，AWS Signer Amazon 預測 AWS Amplify， AWS App Mesh（IAM） AWS App Runner，Amazon 針點，Amazon AppStream 2.0 AWS CodeArtifact，亞馬遜彈性運算雲（亞馬遜 EC2），Amazon Forecast，AWS Identity and Access Management（IAM），亞馬遜針點，亞馬遜數據 Firehose 資源類型。 SageMaker AWS Transfer Family如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 6 月 5 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• cloudfront-s3-origin-access-control-enabled<br>• custom-schema-registry-policy-attached<br>• ec2-client-vpn-not-authorize-all<br>• elasticache-supported-engine-version<br>• macie-status-check<br>• mq-automatic-minor-version-upgrade-enabled<br>• mq-cloudwatch-audit-logging-enabled<br>• netfw-logging-enabled<br>• opensearch-encrypted-at-res<br>• step-functions-state-machine-logging-enabled | 2023 年 5 月 10 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新 Amazon Route 53 Resolver 的 Amazon Elastic Compute Cloud (Amazon EC2) AWS Network Manager、 AWS IoT 無線 AWS Device Farm、AWS Ground Station、、AppFlow、、Amazon、Amazon Redshift、Amazon Pinpoint、 AWS IoT AWS AppConfig、EC2 Image Builder CloudWatch、Amazon SageMaker 執行階段 AWS Panorama、Amazon ECR 和 AWS Audit Manager 資源類型。如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 5 月 5 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到`AWS::NetworkFirewall::TLSInspectionConfiguration` 。如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 5 月 1 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | 該`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策現在為 Amazon 託管工作流程授予 AWS Amplify，AWS App Mesh CloudFront AWS CodeArtifact，Amazon 彈性計算雲，Amazon 肯德拉，Amazon Macie，Amazon 路線 53，Amazon SageMaker，Amazon Pinpoint AWS Transfer Family， AWS 彈性中心， AWS Migration Hub Amazon CloudWatch， AWS Directory Service 和。 AWS App Runner AWS WAF如需詳細資訊，請參閱 AWS Config的 AWS 受管政策。 | 2023 年 4 月 13 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• elasticache-auto-minor-version-upgrade-check<br>• elasticache-repl-grp-auto-failover-enabled<br>• elasticache-repl-grp-encrypted-at-rest<br>• elasticache-repl-grp-encrypted-in-transit<br>• elasticache-repl-grp-redis-auth-enabled<br>• elasticache-subnet-group-check<br>• cloudfront-s3-origin-non-existent-bucket | 2023 年 4 月 10 日 |
| 提高組織一致性套件的服務限制 | 在此版本中，在所有組織一致性套件中，每個帳戶 AWS Config 支援 350 個 AWS Config 規則。如需詳細資訊，請參閱 服務限制。 | 2023 年 4 月 3 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• acm-certificate-rsa-check<br>• appsync-associated-with-waf<br>• appsync-logging-enabled<br>• elasticache-rbac-auth-enabled<br>• mq-no-public-access<br>• netfw-multi-az-enabled<br>• ses-malware-scanning-enabled<br>• eks-cluster-logging-enabled<br>• appsync-cache-encryption-at-rest | 2023 年 4 月 3 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用將組態變更記錄 AWS Config 到新的 Amazon AppStream 2.0、 AWS Auto Scaling、Amazon Connect Amazon 彈性運算雲端、Amazon EventBridge、Kinesis 視訊串流 HealthLake、Lookout for Vision AWS IoT TwinMaker 、網路管理員、亞馬遜精準點、Amazon Route 53 應用程式復原控制器和 AWS RoboMaker 資源類型。如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 4 月 3 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | 該`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策現在為 Amazon，Amazon AppStream 2.0，Amazon，Amazon AppFlow AWS App Runner，Amazon 彈性計算雲（Amazon CloudWatch EC2）CloudFront，Amazon EC2 AWS Device Farm，Amazon Forecast，（IAM），Amazon CloudWatch MemoryDB 為 Redis，Amazon Pinpoint AWS IoT，Amazon 關係數據庫服務 AWS Identity and Access Management（亞馬遜 RDS），亞馬遜 Redshift 和亞馬遜授予其他許可。 AWS CloudFormation AWS CodeArtifact AWS CodeCommit AWS Ground Station AWS Network Manager AWS Panorama SageMaker如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 3 月 30 日 |
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 原則和原`AWS_ConfigRole` 則現在會授與的其他權限 AWS Audit Manager。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 3 月 3 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新的 Amazon AWS Elemental MediaPackage、 EventBridge AWS IoT、(Amazon 簡單儲存服務 (Amazon S3)、亞馬遜彈性運算雲端 (Amazon EC2)、亞馬遜 Lookout for Metrics、Amazon Lex、AWS Budgets、 AWS Device Farm、亞馬遜 CodeGuru 審閱者和 AWS RoboMaker 資源類型。 Amazon Route 53 Resolver如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 3 月 2 日 |
| 安全 IAM 更新 | AWS Config 現在會追蹤`AWSConfigMultiAccountSetupPolicy` 政策的變更。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 2 月 27 日 |
| AWS Config 依區域可用性的資源涵蓋 | 在此版本中， AWS Config 提供每個支援資源類型的「區域」資訊。如需哪些區域支援哪些資源類型的資訊，請參閱《依區域可用性列出的資源涵蓋範圍》。 | 2023 年 2 月 20 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新的 Amazon Interactive Video Service (Amazon IVS)、Amazon 簡單儲存服務 (Amazon S3) AWS Glue、Amazon Elastic Kubernetes Service (亞馬遜 EKS) AWS IoT、Amazon Relational Database Service 服務 (Amazon RDS) 以及 Apache Flink 資源類型的受管服務。如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 2 月 7 日 |
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策現在為 Apache 氣流，Amazon AppStream 2.0，Amazon CodeGuru 審閱者 AWS IoT，Amazon Kinesis 視頻流 AWS HealthLake，Amazon 路線 53 應用程序恢復控制器 AWS Device Farm，Amazon Elastic Compute Cloud (Amazon EC2) 針點 AWS Identity and Access Management（IAM），Amazon 和 Amazon GuardDuty 日誌授予其他許可。 CloudWatch 如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 2 月 1 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | 作為安全最佳實務，`ConfigConformsServiceRolePolicy` 政策現在移除 `config:DescribeConfigRules` 的廣泛資源層級許可。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 1 月 12 日 |
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策現在為 Prometheus、、、、()、 AWS Audit Manager Amazon 彈性運算雲 AWS Database Migration Service (Amazon EC2 AWS DMS)、AWS Directory Service、、Amazon Lightsail、Amazon AWS Glue AWS IoT、亞馬遜路線 53 應用程式恢復控制器 AWS Elemental MediaPackage AWS Network Manager QuickSight AWS Resource Access Manager、亞馬遜簡單儲存服務 (Amazon S3) 和 Amazon Timestream 授予其他許可。 AWS Device Farm如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2023 年 1 月 10 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新的 Amazon MQ、、、Amazon EventBridge 架構描述 AWS AppConfig AWS Cloud9、亞馬遜 Fraud Detector、、、、Amazon Lightsail AWS IoT AWS IoT Analytics、 AWS Elemental MediaPackage (MediaPackage)、Amazon Route 53 應用程式復原控制器和 AWS Transfer Family 資源類型的組態變更。 AWS Resilience Hub 如需詳細資訊，請參閱《支援的資源類型》。 | 2023 年 1 月 5 日 |
| AWS Config 規則資源涵蓋 | 在此版本中， AWS Config 顯示增加 AWS Config 受管規則數目的資源類型涵蓋範圍。 | 2022 年 12 月 21 日 |
| AWS Config 規則可探索性 | 在此版本中， AWS Config 支援「按評估模式排序的 AWS Config 受管規則清單」、「按觸發類型排序的 AWS Config 受管理規則清單」和「依區域可用性分類的 AWS Config 受管規則清單」的頁面。 | 2022 年 12 月 21 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新下列一致性套件：<br>• K-ISMS 的操作最佳實務<br>• NIST 800 171 的操作最佳實務<br>• PCI DSS 3.2.1 的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) 高的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) 中的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) 低的操作最佳實務<br>• NZISM 的操作最佳實務<br>• NIST 800-53 修訂版 5 的操作最佳實務 | 2022 年 12 月 19 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• api-gwv2-access-logs-enabled<br>• api-gwv2-authorization-type-configured<br>• cloudfront-security-policy-check<br>• ec2-launch-template-public-ip-disabled<br>• elastic-beanstalk-logs-to-cloudwatch<br>• sagemaker-notebook-instance-inside-vpc<br>• sagemaker-notebook-instance-root-access-check<br>• security-account-information-provided<br>• storagegateway-resources-protected-by-backup-plan<br>• wafv2-rulegroup-not-empty<br>• wafv2-webacl-not-empty | 2022 年 12 月 9 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新的 Amazon CloudWatch RUM、Amazon、Amazon EventBridge GuardDuty、亞馬遜簡單電子郵件服務 (Amazon SES)、 AWS Backup AWS DataSync、和 AWS Fault Injection Service (AWS FIS) 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 12 月 9 日 |

| | | |
|---|---|---|
| AWS Config 主動合規 | 在此版本中，AWS Config 支援在資源佈建之前主動檢查規 AWS Config 則是否符合性的能力。這可讓您在建立或更新資源的組態設定之前評估這些設定。用 AWS Config 於追蹤對資源所做的組態變更 (預先佈建或佈建後)，並檢查您的資源是否符合您所需的組態。<br><br>新增了下列資料類型：<br><br>• GetResourceEvaluationSummary<br>• StartResource評估<br>• ListResource評估<br><br>更新了下列資料類型：<br><br>• DescribeConfigRulesFilters<br>• GetComplianceDetailsBy資源<br>• EvaluationResult限定符<br>• EvaluationMode配置<br><br>更新了《開發人員指南》中的下列頁面：<br><br>• AWS Config 規則的元件<br>• AWS Config 規則的評估模式與觸發程式型態<br>• AWS Config 受管規則<br>• AWS Config 自訂規則<br>• 管理您的 AWS Config 規則 | 2022 年 11 月 28 日 |

| | | |
|---|---|---|
| 配置記錄器的漂移偵測作為 AWS Config 組態項目 (CI) | 在此版本中，會追 AWS Config 蹤組態錄製程式的所有變更，以指出組態錄製程式的狀態是否與先前狀態不同或已漂移；例如，如果您已經停止或啟 AWS Config 動組態錄製程式，或者您已刪除或解除安裝組態錄製程式，則是否已啟用可追蹤的資源類型更新。資`AWS::Config::ConfigurationRecorder` 源類型是系統資源類型， AWS Config 且此資源類型的記錄預設會在所有支援的區域中啟用。`AWS::Config::ConfigurationRecorder` 資源型態的記錄不會收取額外的費用。如需詳細資訊，請參閱《組態記錄器的漂移偵測》。 | 2022 年 11 月 18 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新的 EC2 Image Builder AWS IoT Events、、AWS Cloud Map、Amazon Route 53 應用程式復原控制器和 Amazon Elastic Container Registry (Amazon ECR) 資源類型的組態變更。 AWS DataSync AWS Glue如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 11 月 8 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 原則和原`AWS_ConfigRole` 則現在會授與的其他權限 AWS CloudFormation。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 11 月 7 日 |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援下列一致性套件：<br>• 刑事司法資訊服務 (CJIS) 的操作最佳實務<br>• Amazon 的安全最佳實踐 SageMaker<br>• Amazon Elastic Container Registry 的安全最佳實務<br><br>更新了下列一致性套件：<br>• MAS TRMG 的操作最佳實務<br>• NCSC 網路評估架構的操作最佳實務<br>• NCSC 雲端安全原則的操作最佳實務 | 2022 年 10 月 27 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在授予額外的許可 AWS Certificate Manager, Amazon 管理工作流程 Apache 氣流 AWS Amplify AWS AppConfig,, Amazon Keyspaces, Amazon CloudWatch, Amazon Elastic Compute Cloud (Amazon EC2), 亞 Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector EventBridge AWS Fault Injection Service, Amazon FSx, Amazon, Amazon Location Service GameLift, Amazon Lex 克斯 AWS IoT, Amazon Lightsail, Amazon Pinpoint, Amazon, Amazon 關係 AWS Glue DataBrew AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight資料庫服務 (Amazon RDS), Amazon 重新認知,, Amazon 路線 53 AWS RoboMaker AWS Resource Groups, 亞馬遜 Simple Storage Service (Amazon S3), AWS Cloud Map和. AWS Security Token Service如需詳細資訊，請參閱 AWS Config的 AWS 受管政策。 | 2022 年 10 月 19 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新的 Amazon Elastic Compute Cloud (Amazon EC2)、亞馬遜簡易電子郵件服務 (Amazon SES) 和 AWS DataSync 資源類型的組態變更。 AWS AppConfig AWS Cloud Map如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 10 月 6 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可 AWS Config 以使用記錄對新 Amazon GuardDuty、Amazon SageMaker AWS AppSync AWS Cloud Map、和 AWS DataSync 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 10 月 4 日 |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 更新了 S WIFT CSP 一致性套件的最佳營運作方式。 | 2022 年 10 月 4 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，AWS Config 支援下列一致性套件：<br>• CMMC 2.0 第 1 級的操作最佳實務<br>• CMMC 2.0 第 2 級的操作最佳實務<br><br>更新了下列一致性套件：<br>• Amazon API Gateway 的操作最佳實務<br>• AWS Well-Architected 架構可靠性支柱的營運最佳實務<br>• Well-Architec AWS ted 的架構安全性支柱的營運最佳實務<br>• CMMC 第 1 級的操作最佳實務<br>• CMMC 第 2 級的操作最佳實務<br>• CMMC 第 3 級的操作最佳實務<br>• CMMC 第 4 級的操作最佳實務<br>• CMMC 第 5 級的操作最佳實務<br>• FFIEC 的操作最佳實務<br>• FedRAMP (低) 的操作最佳實務<br>• MAS Notice 655 的操作最佳實務<br>• NBC TRMG 的操作最佳實務 | 2022 年 9 月 30 日 |

| | | |
|---|---|---|
| | • NIST 800 172 的操作最佳實務 | |
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 原則和原`AWS_ConfigRole` 則現在會授與的其他權限 AWS Glue。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 9 月 14 日 |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援 SWIFT CSP 一致性套件的最佳營運作方式。 | 2022 年 9 月 9 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | AWSConfigServiceRolePolicy 政策和政AWS_ConfigRole 策現在為 Amazon，Amazon，Amazon CloudWatch 朗姆酒 AppFlow CloudWatch，Amazon CloudWatch Synthetics 料，Amazon Connect 客戶檔案，Amazon Connect 語音 ID，Amazon DevOps 大師，Amazon 彈性計算雲（Amazon EC2），Amazon EC2 Auto Scaling，Amazon EMR，Amazon EventBridge 模式 EventBridge，Amazon Fraud Detector Amazon FinSpace，Amazon GameLift，Amazon 交互式視頻服務（亞馬遜 IVS），亞馬遜託管服務 Apache，亞馬遜 Flink，Amazon LexLightsail, Amazon 定 Location Service, Amazon Lookout for Equipment 瞭望, Amazon 觀測指標, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon 敏捷 StudioAmazon Pinpoint, Amazon QuickSight, Amazon 路線 53 應用程序恢復控制器 Amazon Route 53 Resolver,, Amazon 簡單存儲服務（亞馬遜 S3），亞馬遜 SimpleDB, 亞馬遜簡單電子郵件服務（Amazon | 2022 年 9 月 7 日 |

SES ） AWS AppConfig AWS AppSync AWS Auto Scaling, Amazon Timestream AWS Backup, AWS Budgets, AWS Cost Explorer, AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events、 AWS IoT SiteWise AWS IoT TwinMaker 、 AWS Lake Formation、 AWS License Manager、 AWS Resilience Hub AWS Signer、和 AWS Transfer Family。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，AWS Config 支援下列一致性套件：<br>• Amazon 的操作最佳實踐 CloudWatch<br>• 德國雲端運算合規控制目錄 (C5) 的操作最佳實務<br>• IRS 1075 的操作最佳實務<br><br>更新了下列一致性套件：<br>• AWS Control Tower Detective 護衛合規包<br>• CISA Cyber Essentials 的操作最佳實務<br>• ENISA 中小企業網路安全指南的操作最佳實務<br>• FDA 標題 21 CFR 操作最佳實務第 11 部分<br>• FedRAMP (適中) 的操作最佳實務<br>• HIPAA 安全的操作最佳實務<br>• NIST 隱私權架構 1.0 版的操作最佳實務<br>• NYDFS 23 的操作最佳實務<br>• RBI 城市合作銀行 (UCB) 網路安全架構的操作最佳實務<br>• RBI MD-ITF 的操作最佳實務 | 2022 年 8 月 31 日 |

| | | |
|---|---|---|
| 開始使用 AWS Config 和自訂一致性套件更新 | 在此版本中， AWS Config 更新「開始使用」 AWS Config 和「使AWS Config 用主控台進行設定」頁面，並引入一鍵式設定和手動設定頁面。 AWS Config 也會更新「自訂一致性套件」 頁面，並提供如何從頭開始建立一致性套件 YAML 檔案的逐步解說。 | 2022 年 8 月 25 日 |
| AWS Systems Manager 文件 (SSM 文件) 與一致性套件整合 | 在此版本中，您可以使用 SSM 文件建立一致性套件範本。如需 SSM 文件的詳細資訊，請參閱《 AWS Systems Manager 使用者指南》中的《AWS Systems Manager 文件》。<br><br>更新了下列資料類型：<br><br>• PutConformance包<br>• ConformancePack細節<br>• 模板 DocumentDetails<br><br>更新了《開發人員指南》中的下列頁面：<br><br>• 使用主控台部署一致性套件 AWS Config<br>• 使用 AWS 指令行介面部署一致性套件 | 2022 年 8 月 24 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | 政`AWSConfigServiceRolePolicy` 策和`AWS_ConfigRole` 政策現在為 Amazon Simple Email Service (Amazon SES) 和 AWS Cloud Map. AWS DataSync如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 8 月 22 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新的 Amazon 雅典娜、Amazon Detective、Amazon、亞馬遜路線 53 SageMaker、()、 AWS Database Migration Service (AWS DMS) 和亞馬遜簡單電子郵件服務 (Amazon SES) 資源類型的組態變更。 AWS Glue AWS Key Management Service AWS KMS如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 8 月 16 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新下列一致性套件：<br>• NIST 1800 25 的操作最佳實務<br>• NIST 800 181 的操作最佳實務<br>• ABS CCIG 2.0 標準工作負載的操作最佳實務<br>• ABS CCIG 2.0 重大工作負載的操作最佳實務<br>• ACSC Essential 8 的操作最佳實務<br>• ACSC ISM 的操作最佳實務<br>• APRA CPG 234 的操作最佳實務<br>• 獨聯體 AWS 基金會基準 v1.4 級 1 的運營最佳實踐<br>• 獨聯體 AWS 基金會基準第 1.4 版第 2 級的運營最佳實踐<br>• BNM RMiT 的操作最佳實務<br>• NIST CSF 的操作最佳實務 | 2022 年 8 月 1 日 |

| | | |
|---|---|---|
| 一致性套件的合規分數 | 在此版本中，會 AWS Config 引入一致性套件的相容性分數，提供您一致性套件相容性狀態的高階檢視。您可以使用合規分數來識別、調查和了解一致性套件中的合規程度。合規分數是一致性套件中合規規則與合規資源組合數目，相較於一致性套件中可能規則與可能資源組合總數的百分比。<br><br>更新了下列資料類型：<br><br>• ListConformancePackCompliance得分<br>• ConformancePackComplianceScore<br><br>更新了《開發人員指南》中的下列頁面：<br><br>• 檢視 AWS Config 儀表板<br>• 在一致性套件儀表板中檢視合規資料<br>• 管理一致性套件 (API) | 2022 年 7 月 26 日 |
| 安全 IAM 更新 | 該`ConfigConformsServiceRolePolicy` 政策現在授予將指標資料點發佈到 Amazon 的權限 CloudWatch。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 7 月 25 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在為 Amazon 彈性容器服務（Amazon ECS），Amazon，Amazon FSx，Amazon 管理服務授予 Apache Flink ElastiCache EventBridge，Amazon Location Service，Amazon 卡夫卡，Amazon Rekognition，Amazon 簡單存儲服務（Amazon S3），亞馬遜簡單電子郵件服務（亞馬遜 SES）的管理流 QuickSight，亞馬遜 AWS RoboMaker，亞馬遜 Rekognition，亞馬遜簡單存儲服務（亞馬遜 S3） AWS Amplify AWS AppConfig AWS AppSync，亞馬遜簡單電子郵件服務 AWS IAM Identity Center（亞馬遜 SES） AWS Billing Conductor， AWS DataSync AWS Firewall Manager AWS Glue和 Elastic Load Balancing。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 7 月 15 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新的 Amazon Elastic Compute Cloud (Amazon EC2) 資源類型。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 7 月 8 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使用記錄 AWS Config 對新 AWS Global Accelerator 資源類型的配置變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 7 月 5 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• autoscaling-launch-template<br>• ecs-task-definition-log-configuration<br>• ecs-awsvpc-networking-enabled<br>• nlb-cross-zone-load-balancing-enabled | 2022 年 7 月 1 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，AWS Config 支援下列一致性套件：<br>• 加拿大網路安全中心 (CCCS) 中型雲端控制設定檔的操作最佳實務<br>• Gramm Leach Bliley Act (GLBA) 的操作最佳實務<br>• GxP EU Annex 11 的操作最佳實務<br>• Amazon Elastic Kubernetes Service (Amazon EKS) 的安全最佳實務<br>• Amazon Relational Database Service (Amazon RDS) 的安全最佳實務<br>• 安全性最佳做法 AWS Lambda<br><br>更新了下列一致性套件：<br>• AI 和 ML 的操作最佳實務<br>• Amazon DynamoDB 的操作最佳實務<br>• CIS Critical Security Controls v8 IG1 的操作最佳實務<br>• CIS Critical Security Controls v8 IG2 的操作最佳實務<br>• CIS Critical Security Controls v8 IG3 的操作最佳實務<br>• HIPAA 安全的操作最佳實務 | 2022 年 6 月 30 日 |

| | | |
|---|---|---|
| | • NIST 800-53 修訂版 5 的操作最佳實務<br>• NIST CSF 的操作最佳實務 | |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄對新 Amazon SageMaker 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 6 月 29 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到 Apache 卡夫卡 (Amazon MSK)、Amazon 路線 53、Amazon、(IAM 存取分析器) WorkSpaces AWS Batch、 AWS Identity and Access Management Access Analyzer () 和 Elastic Load Balancing 資源類型的新 Amazon 受管串流。AWS Database Migration Service AWS DMS AWS Step Functions如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 6 月 14 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• aurora-last-backup-recovery-point-created<br>• dynamodb-last-backup-recovery-point-created<br>• ebs-last-backup-recovery-point-created<br>• ec2-last-backup-recovery-point-created<br>• efs-last-backup-recovery-point-created<br>• fsx-last-backup-recovery-point-created<br>• rds-last-backup-recovery-point-created<br>• s3-last-backup-recovery-point-created<br>• storagegateway-last-backup-recovery-point-created<br>• virtualmachine-last-backup-recovery-point-created | 2022 年 6 月 13 日 |

| | | |
|---|---|---|
| AWS Config 與整合 AWS Security Hub | 在此版本中，您可以將 AWS Config 受管理和自訂規則評估的結果視為中 AWS Security Hub的發現項目。Security Hub 會將規則評估轉換為調查結果，其中提供受影響資源的詳細資訊，例如 Amazon Resource Name (ARN) 和建立日期。這些調查結果可與其他 Security Hub 調查結果一起檢視，以提供安全狀態的完整概觀。如需詳細資訊，請參閱《將規則評估傳送至 Security Hub》 | 2022 年 6 月 7 日 |
| 安全 IAM 更新 | 該`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策現在為 Amazon Athena，Amazon Detective，Amazon，亞 Amazon Macie GuardDuty，亞馬遜簡單電子郵件服務（Amazon SES） AWS Glue， AWS Resource Access Manager （AWS RAM）和 AWS IAM Identity Center授予其他許可。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 5 月 31 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援下列一致性套件：<br>• Amazon Elastic Container Service (Amazon ECS) 的安全最佳實務<br>• Amazon Elastic File System (Amazon EFS) 的安全最佳實務<br>• Amazon 的安全最佳實踐 CloudFront<br>• 安全性最佳做法 AWS Auto Scaling<br>• 安全性最佳做法 AWS Network Firewall<br>• 安全性最佳做法 AWS Secrets Manager | 2022 年 5 月 31 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄對新 Amazon SageMaker 和 AWS Step Functions 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 5 月 26 日 |
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新 NERC CIP BCSI 一致性套件的營運最佳作法。 | 2022 年 5 月 20 日 |

| | | |
|---|---|---|
| AWS Config 規則的元件 | 在此版本中， AWS Config 介紹了「AWS Config 規則元件」頁面。此頁面討論規則定義的結構、規則中繼資料，以及如何使用規則開發套件 (RDK) 和 AWS Config 規則開發套件程式庫 (RDKLib) 使用 Python 撰寫 AWS Config 規則的最佳作法。 | 2022 年 5 月 9 日 |
| 提高組織一致性套件的服務限制 | 在此版本中，在所有組織一致性套件中，每個帳號都 AWS Config 支援 180 個 AWS Config 規則。如需詳細資訊，請參閱 服務限制。 | 2022 年 5 月 6 日 |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援下列一致性套件：<br>• Amazon OpenSearch 服務的安全最佳實踐<br>• Amazon Redshift 的安全最佳實務<br>• 安全性最佳做法 AWS CloudTrail<br>• 安全性最佳做法 AWS CodeBuild<br>• 安全性最佳做法 AWS WAF | 2022 年 4 月 29 日 |
| AWS Config 更新受管規則 | 透過此版本， AWS Config 支援 S3 資源依備份計畫受管理規則進行保護。 | 2022 年 4 月 11 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 原則和原`AWS_ConfigRole` 則現在授與其他權限以取得有關所有或指定 AWS CloudTrail 事件資料存放區 (EDS) 的資訊、取得有關全部或指定 AWS CloudFormation 資源的資訊、取得 DynamoDB 加速器 (DAX) 參數群組或子網路群組的清單、取得目前存取區域中帳戶的 AWS Database Migration Service (AWS DMS) 複寫工作的相關資訊，以及取得指定類型的所有原則清單。 AWS Organizations 如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 4 月 7 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• alb-desync-mode-check<br>• autoscaling-capacity-rebalancing<br>• autoscaling-launchconfig-requires-imdsv2<br>• autoscaling-launch-config-hop-limit<br>• autoscaling-multiple-instance-types<br>• clb-desync-mode-check<br>• ecs-container-insights-enabled<br>• ecs-fargate-latest-platform-version<br>• netfw-policy-default-action-fragment-packets<br>• netfw-policy-default-action-full-packets<br>• netfw-policy-rule-group-associated<br>• redshift-audit-logging-enabled<br>• s3-lifecycle-policy-check<br>• waf-regional-rule-not-empty<br>• waf-regional-rulegroup-not-empty<br>• waf-regional-webacl-not-empty<br>• vpc-peering-dns-resolution-check | 2022 年 4 月 4 日 |

| | | |
|---|---|---|
| AWS Config 自訂原則規則 | 在此版本中，AWS Config 可讓您使用 AWS CloudFormation 安全警衛 (警衛) 建立 AWS Config 自訂原則規則。Guard 是一種 policy-as-code 語言，可讓您撰寫由強制執行的政策，AWS Config 而不需要建立 Lambda 函數來管理自訂規則。使用安全警衛策略編寫的規則可以從 AWS Config 控制台或使用規 AWS Config 則 API 來創建。<br><br>更新了《開發人員指南》中的下列頁面：<br><br>• AWS Config 自訂規則<br>• 使用守門員建立 AWS Config 自訂規則<br><br>更新了下列資料類型：<br><br>• 來源<br>• CustomPolicy詳情<br>• ConfigRuleEvaluationStatus<br>• GetCustomRulePolicy<br>• GetOrganizationCustomRule政策<br>• OrganizationCustomPolicyRule元数据 | 2022 年 4 月 4 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使 AWS Config 用記錄對新 Amazon EMR SecurityConfiguration 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 3 月 31 日 |
| AWS Config 更新受管規則 | 透過此版本，可 AWS Config 支援虛擬機器資源保護的逐項備份計劃受管理規則。 | 2022 年 3 月 29 日 |
| AWS Config 與 Amazon CloudWatch 指標集成 | 透過此版本， AWS Config 現在支援 AWS Config 使用「 AWS Config 儀表板」頁面 CloudWatch 中的 Amazon 追蹤您的使用情況和成功指標。CloudWatch 指標是一項監控服務，可提供有關系統效能的資料，包括搜尋、繪製圖表和建立有關 AWS 資源指標的警示功能。從 AWS Config 儀表板，您可以查看哪些流量正在推動您的 AWS Config 使用量，以及工作流程中發生故障的關鍵指標。<br><br>更新了下列頁面：<br><br>• 檢視 AWS Config 儀表板 | 2022 年 3 月 29 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到新的 Amazon GuardDuty 偵測器資源類型。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 3 月 24 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• clb-multiple-az<br>• cloudfront-no-deprecated-ssl-protocols<br>• cloudfront-traffic-to-origin-encrypted<br>• cloudwatch-alarm-action-enabled-check<br>• ec2-no-amazon-key-pair<br>• ec2-paravirtual-instance-check<br>• ec2-token-hop-limit-check<br>• ec2-transit-gateway-auto-vpc-attach-disabled<br>• ecr-private-lifecycle-policy-configured<br>• efs-access-point-enforce-root-directory<br>• efs-access-point-enforce-user-identity<br>• elbv2-multiple-az<br>• kinesis-stream-encrypted<br>• redshift-default-db-name-check<br>• s3-event-notifications-enabled<br>• sns-topic-message-delivery-notification-enabled<br>• waf-global-rulegroup-not-empty<br>• waf-global-rule-not-empty | 2022 年 3 月 23 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新下列一致性套件：<br>• CIS Critical Security Controls v8 IG1 的操作最佳實務<br>• CIS Critical Security Controls v8 IG2 的操作最佳實務<br>• CIS Critical Security Controls v8 IG3 的操作最佳實務<br>• Well-Architec AWS ted 的架構安全性支柱的營運最佳實務<br>• Esquema Nacional de Seguridad (ENS) 低的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) 中的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) 高的操作最佳實務<br>• MAS Notice 655 的操作最佳實務<br>• NIST 1800-25 的操作最佳實務 | 2022 年 3 月 16 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和 `AWS_ConfigRole` 政策現在授予 AWS CloudFormation的其他許可。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 3 月 14 日 |
| AWS Config 更新受管規則 | 在此發行版本中，會 AWS Config 更新下列受管規則：<br>• aurora-resources-protected-by-backup-plan<br>• dynamodb-resources-protected-by-backup-plan<br>• ebs-resources-protected-by-backup-plan<br>• ec2-resources-protected-by-backup-plan<br>• efs-resources-protected-by-backup-plan<br>• fsx-resources-protected-by-backup-plan<br>• rds-resources-protected-by-backup-plan | 2022 年 3 月 10 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新 Amazon 彈性容器登錄公用資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 3 月 4 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新 Amazon 彈性運算雲端資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 2 月 28 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• codedeploy-auto-rollback-monitor-enabled<br>• codedeploy-ec2-minimum-healthy-hosts-configured<br>• codedeploy-lambda-allatonce-traffic-shift-disabled | 2022 年 2 月 25 日 |
| AWS Config 更新中的記錄和監控 | 在此版本中， AWS Config 更新「AWS Config 使用 Amazon EventBridge 事件監控」頁面以取代 Amazon CloudWatch 活動的參考資料。Amazon EventBridge 是管理您的活動的首選方式。 CloudWatch 事件和 EventBridge 基礎服務和 API 相同，但 EventBridge 提供了更多的功能。您在 CloudWatch 或中所做的變更都 EventBridge 會顯示在每個主機中。有關更多信息，請參閱 Amazon。 EventBridge | 2022 年 2 月 24 日 |

| | | |
|---|---|---|
| AWS 適用於的 SDK 頁面 AWS Config | 在此版本中， AWS Config 介紹了「AWS Config 搭配 AWS SDK 使用」頁面。 AWS 軟件開發套件（SDK）可用於許多流行的編程語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。 | 2022 年 2 月 24 日 |
| 安全 IAM 角色信任政策更新 | 在此版本中，會 AWS Config 更新 IAM 信任政策聲明，在信任政策中包含安全保護，以限制使用`sourceARN` 和/或 `sourceAccountId` AWS Security Token Service (AWS STS) 操作的存取。這有助於確保 IAM 角色信任政策僅代表預期的使用者和案例存取資源。<br><br>更新了下列頁面：<br><br>• 將 IAM 信任政策新增至您的角色 | 2022 年 2 月 18 日 |

| | | |
|---|---|---|
| 全域資源類型記錄的變更 | AWS Config 現在會變更錄製中記 AWS Config 錄新的全域資源類型的方式。全域資源型態是指不需要您在建立時指定區域的 AWS 資源。在此變更之前，您可以在 AWS Config的所有支援區域中啟用全域資源類型的記錄。在此變更之後，登入錄製的新全域資源類型只能記 AWS Config 錄在服務的主區域中，以及 AWS GovCloud (美國西部) 用於分割區。 AWS GovCloud (US) 您現在只能在其本地區域和 AWS GovCloud (美國西部) 檢視這些新全域資源類型的組態項目。如需在 2022 年 2 月之後上線之全域資源類型的主要區域清單，請參閱《記錄所有支援的資源類型》頁面上的表格。 | 2022 年 2 月 18 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在授予權限，以取得有關 Elastic Beanstalk 環境的詳細資料以及指定 Elastic Beanstalk 組態集的設定說明、取得 OpenSearch 或 Elasticsearch 版本的對應、描述資料庫可用的 Amazon RDS 選項群組，以及取得有關部署組態的資訊。 CodeDeploy 此政策現在也授與權限，可擷取附加至某個 AWS 帳戶指定的替代聯絡人、擷取有關 AWS Organizations 政策的資訊、擷取 Amazon ECR 儲存庫政策、擷取存檔 AWS Config 規則的資訊、擷取 Amazon ECS 任務定義系列清單、列出指定子 OU 或帳戶的根或父組織單位 (OU)，以及列出附加到指定目標根、組織單位或帳戶的政策。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 2 月 10 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• autoscaling-multiple-az<br>• codebuild-project-artifact-encryption<br>• codebuild-project-environment-privileged-check<br>• codebuild-project-logging-enabled<br>• codebuild-project-s3-logs-encrypted<br>• ec2-security-group-attached-to-eni-periodic<br>• ecr-private-image-scanning-enabled<br>• ecr-private-tag-immutability-enabled<br>• ecs-containers-nonprivileged<br>• ecs-containers-readonly-access<br>• ecs-no-environment-secrets<br>• ecs-task-definition-memory-hard-limit<br>• ecs-task-definition-nonroot-user<br>• ecs-task-definition-pid-mode-check<br>• eks-cluster-oldest-supported-version<br>• eks-cluster-supported-version | 2022 年 2 月 10 日 |

| | | |
|---|---|---|
| | • lambda-vpc-multi-az-check<br>• nacl-no-unrestricted-ssh-rdp<br>• netfw-stateless-rule-group-not-empty<br>• rds-cluster-default-admin-check<br>• rds-db-security-group-not-allowed<br>• rds-instance-default-admin-check<br>• redshift-default-admin-check<br>• s3-bucket-acl-prohibited<br>• s3-version-lifecycle-policy-check<br>• waf-global-webacl-not-empty | |
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在授予建立 Amazon 日 CloudWatch誌群組和串流的權限，以及將日誌寫入建立的日誌串流。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2022 年 2 月 2 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• opensearch-access-control-enabled<br>• opensearch-audit-logging-enabled<br>• opensearch-data-node-fault-tolerance<br>• opensearch-encrypted-at-rest<br>• opensearch-https-required<br>• opensearch-in-vpc-only<br>• opensearch-logs-to-cloudwatch<br>• opensearch-node-to-node-encryption-check | 2022 年 1 月 31 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS CodeDeploy 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2022 年 1 月 5 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄對新 Amazon SageMaker 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2021 年 12 月 20 日 |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援下列一致性套件：<br>• ENISA 中小企業網路安全指南的操作最佳實務 | 2021 年 12 月 20 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，AWS Config 支援下列一致性套件：<br>• NIST 800 172 的操作最佳實務<br>• NIST 800 181 的操作最佳實務<br><br>更新了下列一致性套件：<br>• K-ISMS 的操作最佳實務 | 2021 年 11 月 18 日 |
| AWS Config 支援新的一致性套件 | 在此版本中，AWS Config 支援下列一致性套件：<br>• Amazon API Gateway 的操作最佳實務<br>• 下列項目的最佳作業 AWS Backup<br>• CISA Cyber Essentials 的操作最佳實務<br>• 下列項目的最佳作業 DevOps<br>• NIST 隱私權架構 1.0 版的操作最佳實務<br><br>更新了下列一致性套件：<br>• FedRAMP (低) 的操作最佳實務<br>• FedRAMP (適中) 的操作最佳實務 | 2021 年 10 月 29 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使用記錄 AWS Config 對新 Amazon OpenSearch 服務資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2021 年 10 月 12 日 |
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新下列一致性套件：<br>• MAS TRMG 的操作最佳實務 | 2021 年 10 月 12 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新下列一致性套件：<br>• ABS CCIG 2.0 重大工作負載的操作最佳實務<br>• ABS CCIG 2.0 標準工作負載的操作最佳實務<br>• ACSC Essential 8 的操作最佳實務<br>• ACSC ISM 的操作最佳實務<br>• BNM RMiT 的操作最佳實務<br>• CMMC 第 1 級的操作最佳實務<br>• CMMC 第 2 級的操作最佳實務<br>• CMMC 第 3 級的操作最佳實務<br>• CMMC 第 4 級的操作最佳實務<br>• CMMC 第 5 級的操作最佳實務<br>• FDA 標題 21 CFR 操作最佳實務第 11 部分<br>• FFIEC 的操作最佳實務<br>• MAS Notice 655 的操作最佳實務<br>• NBC TRMG 的操作最佳實務<br>• NERC CIP 的操作最佳實務<br>• NIST 800-53 修訂版 5 的操作最佳實務 | 2021 年 9 月 30 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在授予權限，以取得有關 Amazon OpenSearch 服務 (服OpenSearch 務) 網域/網域的詳細資料，以及取得特定 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫參數群組的詳細參數清單。此政策也授予取得 Amazon ElastiCache 快照詳細資訊的權限。如需詳細資訊，請參閱 AWS Config的 AWS 受管政策。 | 2021 年 9 月 8 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄新 Amazon 彈性運算雲端資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2021 年 9 月 7 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，會 AWS Config 更新下列一致性套件：<br>• APRA CPG 234 的操作最佳實務<br>• 獨聯體 AWS 基金會基準 v1.4 級 1 的運營最佳實踐<br>• 獨聯體 AWS 基金會基準第 1.4 版第 2 級的運營最佳實踐<br>• NCSC 雲端安全原則的操作最佳實務<br>• NCSC 網路評估架構的操作最佳實務<br>• NIST 800 171 的操作最佳實務<br>• NIST CSF 的操作最佳實務<br>• RBI 城市合作銀行 (UCB) 網路安全架構的操作最佳實務<br>• RBI MD-ITF 的操作最佳實務<br>• NYDFS 23 的操作最佳實務<br>• PCI DSS 3.2.1 的操作最佳實務 | 2021 年 8 月 30 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• aurora-resources-protected-by-backup-plan<br>• backup-plan-min-frequency-and-min-retention-check<br>• backup-recovery-point-encrypted<br>• backup-recovery-point-manual-deletion-disabled<br>• backup-recovery-point-minimum-retention-check<br>• dynamodb-resources-protected-by-backup-plan<br>• ebs-resources-protected-by-backup-plan<br>• ec2-resources-protected-by-backup-plan<br>• efs-resources-protected-by-backup-plan<br>• fsx-resources-protected-by-backup-plan<br>• rds-resources-protected-by-backup-plan | 2021 年 8 月 20 日 |
| AWS Config 支援新的一致性套件 | 在此版本中，AWS Config 支援下列一致性套件：<br>• NZISM 的操作最佳實務 | 2021 年 8 月 20 日 |

| | | |
|---|---|---|
| 安全 Amazon SNS 政策更新 | `sourceAccountId` 在此版本中，使用服務連結角色包含限制在主題政策中存取`sourceARN` 和/或限制存取的安全保護時，會 AWS Config 更新 Amazon SNS 主題的 IAM 政策聲明。這有助於確保 Amazon SNS 僅代表預期的使用者和案例存取資源。<br><br>更新了下列頁面：<br><br>• Amazon SNS 主題的許可 | 2021 年 8 月 17 日 |
| 安全 AWS Lambda 策略更新 | 在此發行版本中，會 AWS Config 更新 AWS Config 自訂規則的 AWS Lambda 資源型政策，以納入安全性保護，以限制呼叫請求`sourceAccountId` 中的`sourceARN` 存取權限。這有助於確保 AWS Lambda 僅代表預期的使用者和案例存取您的資源。<br><br>更新了下列頁面：<br><br>• AWS::Config::ConfigRule<br>• 為下列項目開發自訂規則 AWS Config | 2021 年 8 月 12 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon Kinesis 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2021 年 8 月 6 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援下列一致性套件：<br><br>• Esquema Nacional de Seguridad (ENS) 高的操作最佳實務<br><br>更新了下列一致性套件：<br><br>• AWS Well-Architected 架構可靠性支柱的營運最佳實務<br>• Well-Architec AWS ted 的架構安全性支柱的營運最佳實務<br>• Esquema Nacional de Seguridad (ENS) 低的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) 中的操作最佳實務<br>• HIPAA 安全的操作最佳實務 | 2021 年 7 月 30 日 |
| AWS Config 自訂規則的範例 AWS Lambda 函數 | 在此發行版本中，在AWS Config 規則的範例函 AWS Lambda 數 (Python) 中 AWS Config 提供 Python 範例函數。 | 2021 年 7 月 29 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和 `AWS_ConfigRole` 政策現在授予許可，以列出日誌群組的標籤、列出狀態機器的標籤，以及列出所有狀態機器。這些原則現在授予許可，以取得有關狀態機器的詳細資訊。這些政策現在還支持 Amazon EC2 Systems Manager（SSM），Amazon 彈性容器註冊表，Amazon FSX，Amazon 數據火狐，阿帕奇卡夫卡 Amazon 託管流（Amazon MSK），Amazon Relational Database Service（Amazon RDS），Amazon 路線 53，Amazon 簡單通知服務， SageMaker等等。 AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2021 年 7 月 28 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS Backup 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2021 年 7 月 14 日 |

| | | |
|---|---|---|
| AWS Config 支援新的一致性套件 | 在此版本中，AWS Config 支援下列一致性套件：<br>• CIS Critical Security Controls v8 IG1 的操作最佳實務<br>• CIS Critical Security Controls v8 IG2 的操作最佳實務<br>• CIS Critical Security Controls v8 IG3 的操作最佳實務<br>• NIST 1800 25 的操作最佳實務 | 2021 年 7 月 9 日 |
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• ssm-document-not-public<br>• s3-account-level-public-access-blocks-periodic | 2021 年 6 月 25 日 |
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• ec2-instance-multiple-eni-check<br>• elbv2-acm-certificate-required<br>• autoscaling-launch-config-public-ip-disabled | 2021 年 6 月 10 日 |

| | | |
|---|---|---|
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 政策和政`AWS_ConfigRole` 策現在授予查看 AWS Systems Manager 文件許可和 IAM Access Analyzer 相關資訊的權限。這些政策現在支援 Amazon Kinesis、Amazon、Amazon EMR ElastiCache、亞馬遜路線 53 和 Amazon Relational Database Service 服務 (Amazon RDS) 的其他 AWS 資源類型。 AWS Network Firewall這些權限變更 AWS Config 允許叫用支援這些資源類型所需的唯讀 API。這些原則現在也支援針對 vpc 內 AWS Config 部受管規則篩選 Lambda @Edge 函數。如需詳細資訊，請參閱 AWS Config的 AWS 受管政策。 | 2021 年 6 月 8 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• elasticsearch-logs-to-cloudwatch<br>• rds-cluster-multi-az-enabled<br>• api-gw-associated-with-waf<br>• iam-policy-no-statements-with-full-access | 2021 年 5 月 19 日 |

| | | |
|---|---|---|
| AWS Config 支援新資源類型 | 在此版本中，您可以使用記錄 AWS Config 對 Amazon Elastic File System 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2021 年 5 月 13 日 |
| 安全 IAM 更新 | 原則和`AWSConfigServiceRolePolicy` 政`AWS_ConfigRole` 策現在會授與允許對 API Gateway AWS Config 進行唯讀 GET 呼叫的權限，以支援 API Gateway 的 Config 規則。這些政策還新增許可，AWS Config 允許叫用 Amazon Simple Storage Service (Amazon S3) 唯讀 API，這些 API 是支援新`AWS::S3::AccessPoint` 資源類型所需的。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2021 年 5 月 10 日 |
| AWS Config 自訂規則 | 更新了《開發人員指南》中的下列頁面：<br>• 開始使用的自訂規則 AWS Config<br>• 為下列項目開發自訂規則 AWS Config | 2021 年 4 月 30 日 |

| | | |
|---|---|---|
| AWS Config 更新受管規則 | 在此發行版本中，AWS Config 支援下列受管規則：<br>• aurora-mysql-backtracking-enabled<br>• ec2-instance-profile-attached<br>• ecs-task-definition-user-for-host-mode-check<br>• no-unrestricted-route-to-igw<br>• rds-automatic-minor-version-upgrade-enabled<br>• redshift-enhanced-vpc-routing-enabled | 2021 年 4 月 15 日 |
| 安全 IAM 更新 | `AWSConfigServiceRolePolicy` 原則和原`AWS_ConfigRole` 則現在會授與檢視 AWS Systems Manager 指定文件相關資訊的權限。這些政策現在還支援 Amazon 彈性檔案系統 AWS Backup、Amazon、Amazon 簡單儲存服務 (Amazon S3) ElastiCache、亞馬遜彈性運算雲 (Amazon EC2)、亞馬遜 Kinesis、亞馬遜和亞馬遜 SageMaker路線 53 的其他 AWS 資源類型。 AWS Database Migration Service這些權限變更 AWS Config 允許叫用支援這些資源類型所需的唯讀 API。如需詳細資訊，請參閱 AWS Config的AWS 受管政策。 | 2021 年 4 月 14 日 |

| | | |
|---|---|---|
| 一致性套件合規作為組態項目 (CI) | 在此版本中，將符合性套件相容性作為組態項目 AWS Config 支援。這可讓您：<br>• 檢視一致性套件合規狀態變更的時間軸<br>• 彙總多個帳戶和區域的一致性套件合規<br>• 使用進階查詢來檢查一致性套件的合規<br><br>更新了下列資料類型：<br>• DescribeAggregateComplianceByConformancePacks<br>• GetAggregateConformancePackComplianceSummary<br><br>更新了《開發人員指南》中的下列頁面：<br>• 在一致性套件儀表板中檢視合規資料<br>• 檢視一致性套件的合規歷史記錄時間軸<br>• 在彙總工具儀表板中檢視合規資料<br>• 查詢資 AWS 源的目前組態狀態<br>• 支援的資源類型 | 2021 年 3 月 30 日 |

| | | |
|---|---|---|
| 分頁更新 | 在此版本中， AWS Config 進階查詢功能現在支援包含彙總函式 (例如 COUNT 和 SUM) 的查詢的分頁。您現在可以使用進階查詢，透過分頁取得彙總查詢的完整結果 (先前限制為 500 列)。如需詳細資訊，請參閱查詢資 AWS 源的目前組態狀態 | 2021 年 3 月 26 日 |
| 區域支援 | 在此版本中 AWS Config ，「 AWS Config 規則」現已在亞太區域 (大阪) 區域提供支援。 | 2021 年 3 月 4 日 |
| AWS Config 支援新資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon 彈性容器登錄、Amazon 彈性容器服務和亞馬 Amazon Elastic Kubernetes Service 資源類型的組態變更。如需詳細資訊，請參閱《支援的資源類型》。 | 2021 年 2 月 25 日 |

| | | |
|---|---|---|
| KMS 加密支援 | 在此版本中，您 AWS Config 可以在 S3 儲存貯體交付的物件上使用 KMS 型加密。 AWS Config<br><br>更新了下列資料類型：<br><br>• DeliveryChannel<br>• PutDelivery頻道<br><br>更新了《開發人員指南》中的下列頁面：<br><br>• KMS 金鑰的許可<br>• 指派給的 IAM 角色的許可 AWS Config | 2021 年 2 月 16 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br><br>• secretsmanager-secret-periodic-rotation<br>• secretsmanager-secret-unused<br>• secretsmanager-using-cmk | 2021 年 2 月 16 日 |
| 已儲存的查詢區域支援 | 在此版本中， AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域現在支援已儲存的查詢。 | 2021 年 2 月 15 日 |
| 多帳戶多區域資料彙總區域支援 | 在此版本中，非洲 (開普敦) 和歐洲 (米蘭) 區域現在支援多帳戶多區域資料彙總。如需詳細資訊，請參閱《多帳戶多區域資料彙總》。 | 2021 年 2 月 15 日 |

| | | |
|---|---|---|
| 進階查詢區域支援 | 在此版本中，非洲 (開普敦) 和歐洲 (米蘭) 區域現在支援進階查詢。如需詳細資訊，請參閱查詢 AWS 資源的目前組態狀態。 | 2021 年 2 月 15 日 |
| AWS Config 文檔歷史記錄通知可通過 RSS 提要 | 您現在可以透過訂閱 RSS 摘要來接收有關 AWS Config 文件更新的通知。 | 2021 年 1 月 1 日 |

# 舊版更新

下表說明 2020 年 12 月 31 日 AWS Config 之前的文件發行歷史記錄。

| 變更 | 描述 | 版本日期 |
|---|---|---|
| 已儲存的查詢支援 | 使用此版本， AWS Config 可讓您儲存查詢。儲存查詢之後，您可以對其進行搜尋、將其複製到查詢編輯器、對其進行編輯，或對其進行刪除。如需如何儲存查詢的詳細資訊，請參閱《使用 SQL 查詢編輯器 (主控台) 查詢》和《使用 SQL 查詢編輯器 (AWS CLI) 進行查詢》。<br><br>如需 API 的詳細資訊，請參閱 AWS Config API 參考：<br><br>• PutStored查詢<br>• GetStored查詢<br>• ListStored查詢<br>• DeleteStored查詢<br><br>另請參閱服務配額。 | 2020 年 12 月 21 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 程序檢查支援 | 在此版本中， AWS Config 支援流程檢查，這是一種 AWS Config 規則類型，可讓您追蹤需要驗證的外部和內部工作，作為一致性套件的一部分。透過程序檢查，您可以列出單一位置的要求與動作合規。<br><br>如需程序檢查的詳細資訊，請參閱AWS Config 符合性套件中的處理檢查主題和PutExternal評估 API。 | 2020 年 12 月 17 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br><br>• api-gw-ssl-enabled<br>• api-gw-xray-enabled<br>• beanstalk-enhanced-health-reporting-enabled<br>• cloudfront-accesslogs-enabled<br>• cloudfront-associated-with-waf<br>• cloudfront-custom-ssl-certificate<br>• elastic-beanstalk-managed-updates-enabled<br>• rds-cluster-iam-authentication-enabled<br>• redshift-cluster-kms-enabled<br>• s3-bucket-level-public-access-prohibited<br>• subnet-auto-assign-public-ip-disabled<br>• vpc-network-acl-unused-check | 2020 年 12 月 17 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支持 AWS Network Firewall | 在此版本中，您可以使 AWS Config 用記錄 AWS Network Firewall FirewallPolicy、 RuleGroup和防火牆資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2020 年 12 月 4 日 |
| 文件更新 | AWS Config 已新增對委派管理員帳戶中整個組織的資源資料彙總支援。您現在可以使用委派的管理員帳戶，從 AWS Organizations 中組織的所有成員帳戶彙總資源組態與合規資料。<br><br>如需詳細資訊，請參閱PutConfiguration彙總器使用主控台設定彙整和註冊委派管理員。 | 2020 年 12 月 4 日 |
| AWS Config 支援新的一致性套件 | • CMMC 第 3 級的操作最佳實務<br>• CMMC 第 4 級的操作最佳實務<br>• CMMC 第 5 級的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) Low 的操作最佳實務<br>• Esquema Nacional de Seguridad (ENS) Medium 的操作最佳實務<br>• NCSC 網路評估架構的操作最佳實務<br>• RBI 城市合作銀行 (UCB) 網路安全架構的操作最佳實務 | 2020 年 10 月 30 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的一致性套件 | • ACSC Essential 8 的操作最佳實務<br>• ACSC ISM 的操作最佳實務<br>• AI 和 ML 的操作最佳實務<br>• 資產管理的操作最佳實務<br>• BCP 和 DR 的操作最佳實務<br>• EC2 的操作最佳實務<br>• K-ISMS 的操作最佳實務<br>• 負載平衡的操作最佳實務<br>• 日誌的操作最佳實務<br>• 監控的操作最佳實務<br>• 無伺服器的操作最佳實務 | 2020 年 10 月 22 日 |
| AWS Config 支援新的一致性套件 | • APRA CPG 234 的操作最佳實務<br>• FedRAMP (低) 的操作最佳實務<br>• MAS Notice 655 的操作最佳實務<br>• NBC TRMG 的操作最佳實務<br>• NCSC 雲端安全原則的操作最佳實務<br>• RBI MD-ITF 的操作最佳實務 | 2020 年 10 月 15 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的一致性套件 | • ABS CCIG 2.0 重大工作負載的操作最佳實務<br>• ABS CCIG 2.0 標準工作負載的操作最佳實務<br>• BNM RMiT 的操作最佳實務<br>• 資料復原的操作最佳實務<br>• 資料湖和分析服務的操作最佳實務<br>• 加密和金鑰管理的操作最佳實務<br>• FDA 標題 21 CFR 操作最佳實務第 11 部分<br>• 可公開存取資源的操作最佳實務<br>• MAS TRMG 的操作最佳實務<br>• NERC CIP BCSI 的操作最佳實務<br>• NYDFS 23 的操作最佳實務 | 2020 年 10 月 8 日 |
| AWS Config 支援新的一致性套件 | • AWS Well-Architected 架構可靠性支柱的營運最佳實務<br>• Well-Architec AWS ted 的架構安全性支柱的營運最佳實務<br>• CMMC 第 1 級的操作最佳實務<br>• CMMC 第 2 級的操作最佳實務<br>• 運算服務的操作最佳實務<br>• 資料庫服務的操作最佳實務<br>• 管理與控管服務的操作最佳實務<br>• 聯網和內容交付服務的操作最佳實務<br>• 安全、身分及合規服務的最佳實務<br>• 儲存服務的操作最佳實務 | 2020 年 10 月 26 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的一致性套件 | • FedRAMP (適中) 的操作最佳實務<br>• FFIEC 的操作最佳實務<br>• HIPAA 安全的操作最佳實務<br>• NIST 800-53 修訂版 4 的操作最佳實務<br>• NIST 800 171 的操作最佳實務 | 2020 年 9 月 28 日 |
| 文件更新 | 更新了下列一致性套件主題。<br>• 必要條件<br>• 使用 AWS Config 主控台部署一致性套件<br>• 管理組織中所有帳戶的一致性套件 | 2020 年 9 月 28 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• iam-customer-policy-blocked-kms-actions<br>• iam-inline-policy-blocked-kms-actions | 2020 年 9 月 17 日 |
| AWS Config 支持第 AWS WAF 2 版 | 在此版本中，您可 AWS Config 以使用記錄對 AWS WAF v2 WebACL、IP set RegexPatternSet、 RuleGroup和 ManagedRuleSet 資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2020 年 9 月 1 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 文件更新 | 《完全存取 AWS Config》新增了有關建立自訂許可以授予完整存取權的注意事項。<br><br>以下規則的文件已更新：<br><br>• s3-bucket-server-side-encryption-enabled<br>• ec2-instance-detailed-monitoring-enabled<br>• ec2-managedinstance-platform-check | 2020 年 8 月 24 日 |
| 文件更新 | 更新了《PCI DSS 3.2.1 的操作最佳實務 》和《NIST CSF 的操作最佳實務 》範本。 | 2020 年 8 月 14 日 |
| 文件更新 | 新增了範例關係查詢。如需詳細資訊，請參閱 範例關係查詢。 | 2020 年 7 月 30 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 文件更新 | 更新了下列資料類型：<br>• ConfigurationAggregator<br>• RemediationConfiguration<br>• DescribeOrganizationConfigRules<br>• GetOrganizationConfigRuleDetailedStatus<br>• DescribeOrganizationConfigRule狀態<br>• DescribeOrganizationConformancePacks<br>• DescribeOrganizationConformancePack狀態<br>• GetOrganizationConformancePackDetailedStatus | 2020 年 7 月 23 日 |
| AWS Config 支援 AWS Systems Manager 資源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS Systems Manager 檔案資料資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2020 年 7 月 9 日 |
| 文件更新 | 更新了《AWS身分識別與存取管理的營運最佳作法》和《PCI DSS 3.2.1 的操作最佳實務 》範本。 | 2020 年 7 月 9 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• account-part-of-organizations<br>• alb-http-drop-invalid-header-enabled<br>• alb-waf-enabled<br>• cloudfront-default-root-object-configured<br>• cloudfront-origin-access-identity-enabled<br>• cloudfront-origin-failover-enabled<br>• EC2_IMDSV2_CHECK<br>• cloudtrail-security-trail-enabled<br>• cw-loggroup-retention-period-check<br>• dax-encryption-enabled<br>• dynamodb-in-backup-plan<br>• ebs-in-backup-plan<br>• ec2-imdsv2-check<br>• efs-in-backup-plan<br>• eks-endpoint-no-public-access<br>• eks-secrets-encrypted<br>• elasticsearch-node-to-node-encryption-check<br>• elb-cross-zone-load-balancing-enabled<br>• elb-tls-https-listeners-only<br>• iam-no-inline-policy-check<br>• rds-cluster-deletion-protection-enabled | 2020 年 7 月 9 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| | • rds-in-backup-plan<br>• rds-instance-deletion-protection-enabled<br>• rds-instance-iam-authentication-enabled<br>• rds-logging-enabled<br>• redshift-backup-enabled<br>• waf-classic-logging-enabled<br>• wafv2-logging-enabled<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | |
| 多帳戶多區域資料彙總區域支援 | 在此版本中，亞太區域 (香港) 和中東 (巴林) 區域現在支援多帳戶多區域資料彙總。如需詳細資訊，請參閱 Multi-Account Multi-Region Data Aggregation 及 多帳戶多區域資料彙整故障診斷。 | 2020 年 7 月 1 日 |
| 進階查詢區域支援 | 在此版本中，亞太區域 (香港) 和中東 (巴林) 區域現在支援進階查詢。如需詳細資訊，請參閱 查詢 AWS 資源目前的組態狀態。 | 2020 年 7 月 1 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 文件更新 | 以下規則的文件已更新：<br>• ec2-managedinstance-association-compliance-status-check<br>• iam-policy-no-statements-with-admin-access<br>• required-tags<br>• restricted-common-ports<br>• rds-snapshots-public-prohibited<br>• s3-bucket-policy-grantee-check | 2020 年 6 月 30 日 |
| 文件更新 | 文件已更新，其中包含的安全性資訊 AWS Config。請參閱中的安全性 AWS Config。 | 2020 年 6 月 24 日 |
| 文件更新 | AWS Control Tower Detective 護衛一致性包範本已更新。如需詳細資訊，請參閱 AWSControl Tower Detective 護衛合規包。 | 2020 年 6 月 4 日 |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援 NIST CSF 一致性套件的作業最佳作法。如需詳細資訊，請參閱 NIST CSF 的操作最佳實務 。 | 2020 年 5 月 29 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• dynamodb-pitr-enabled<br>• dynamodb-table-encrypted-kms<br>• ec2-ebs-encryption-by-default<br>• rds-snapshot-encrypted<br>• redshift-require-tls-ssl<br>• s3-bucket-default-lock-enabled<br>• s3-default-encryption-kms<br>• securityhub-enabled<br>• sns-encrypted-kms<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2020 年 5 月 28 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 委派的管理員支援 | 在此版本中，除了管理帳戶之外，您還可以從組織中的任何委派成員帳戶部署 AWS Config 規則和一致性套件。<br><br>如需 API 的詳細資訊，請參閱 AWS Config API 參考：<br><br>• PutOrganizationConfigRule<br>• PutOrganizationConformancePack<br>• DescribeOrganizationConfigRules<br>• GetOrganizationConfigRuleDetailedStatus<br>• DescribeOrganizationConfigRule狀態<br>• DeleteOrganizationConfigRule<br>• DeleteOrganizationConformancePack<br>• DescribeOrganizationConformancePacks<br>• DescribeOrganizationConformancePack狀態<br>• GetOrganizationConformancePackDetailedStatus<br><br>如需詳細資訊，請參閱 服務配額。 | 2020 年 5 月 27 日 |
| AWS Config 規則區域支援 | 在此版本中，非洲（開普敦）和歐洲（米蘭）地區支持的 AWS Config 規則很少。如需規則及其支援區域的詳細清單，請參閱AWS Config 受管規則清單。 | 2020 年 4 月 28 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的一致性套件 | 在此版本中， AWS Config 支援兩個符合性套件。<br>• AWS Control Tower Detective 護衛合規包<br>• CIS 的操作最佳實務<br><br>如需詳細資訊，請參閱 一致性套件範例範本。 | 2020 年 4 月 22 日 |
| AWS Config 支援 AWS Secrets Manager | 在此發行版本中，您可以用 AWS Config 來記錄 Secrets Manager 碼的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2020 年 4 月 20 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• secretsmanager-rotation-enabled-check<br>• secretsmanager-scheduled-rotation-success-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2020 年 4 月 16 日 |
| 一致性套件區域支援 | 在此版本中，亞太區域 (香港) 和中東 (巴林) 現在支援一致性套件。如需詳細資訊，請參閱 Conformance Packs。 | 2020 年 4 月 8 日 |
| 文件更新 | AWS Config 此開發人員指南中提供了限制。如需詳細資訊，請參閱 服務配額。 | 2020 年 4 月 8 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 文件更新 | 透過 AWS CloudFormation 登錄管理的協力廠商資源 (也就是建立/更新/刪除) 會自動追蹤為組態項目。 AWS Config 如需詳細資訊，請參閱 記錄第三方資源的組態。 | 2020 年 3 月 30 日 |
| 文件更新 | 受 AWS Config 管規則會更新以包含 AWS 區域 資訊。如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2020 年 3 月 27 日 |
| AWS Config 支援 Amazon SNS 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon SNS 主題的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2020 年 3 月 6 日 |
| 多帳戶多區域資料彙總區域支援 | 在此版本中，歐洲 (斯德哥爾摩) 區域現在支援多帳戶多區域資料彙整。如需詳細資訊，請參閱 Multi-Account Multi-Region Data Aggregation。 | 2020 年 3 月 5 日 |
| 進階查詢區域支援 | 在此版本中，歐洲 (斯德哥爾摩) 區域現在支援進階查詢。如需詳細資訊，請參閱 查詢 AWS 資源目前的組態狀態。 | 2020 年 3 月 5 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 可讓您使用組態彙總器執行進階查詢 | 在此版本中， AWS Config 新增支援以資源組態屬性與組態彙總工具執行進階查詢，讓您能夠跨多個帳戶和區域執行相同的查詢。如需詳細資訊，請參閱 查詢 AWS 資源目前的組態狀態。<br><br>在此版本中， AWS Config 新增 `SelectAggregateResourceConfig` API。如需詳細資訊，請參閱 AWS Config API 參考SelectAggregateResourceConfig中的： | 2020 年 2 月 28 日 |
| AWS Config 支援 Amazon SQS 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon SQS 佇列的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2020 年 2 月 13 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS CloudFormation 支援一致性套件 | 在此版本中，已新增對下列資源的 AWS CloudFormation 支援：`AWS::Config::ConformancePack` 和`OrganizationConformancePack` 。<br>• AWS::Config::ConformancePack<br>使用資`AWS::Config::ConformancePack` 源建立「一致性套件」，該套件是一組 AWS Config 規則，可輕鬆部署在帳號、區域以及整 AWS 個組織中。<br>• AWS::Config::OrganizationConformance包<br>使用資`AWS::Config::OrganizationConformancePack` 源建立包含下列相關資訊的「組織一致性套件」 在成員帳戶中 AWS Config 建立的一致性套件。 | 2020 年 2 月 13 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• api-gw-execution-logging-enabled<br>• ec2-stopped-instance<br>• elasticache-redis-cluster-automatic-backup-check<br>• emr-master-no-public-ip<br>• guardduty-non-archived-findings<br>• rds-enhanced-monitoring-enabled<br>• s3-account-level-public-access-blocks<br>• sagemaker-endpoint-configuration-kms-key-configured<br>• service-vpc-endpoint-enabled<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2019 年 12 月 20 日 |
| 記錄自訂資源類型的組態 | 在此版本中， AWS Config 引入了對自訂資源類型記錄組態的支援。您可以將協力廠商資源的組態資料發佈到中， AWS Config 並使用 AWS Config 主控台和 API 檢視和監視資源清查和組態歷程記錄。如需詳細資訊，請參閱 記錄第三方資源的組態。<br><br>如需 API 的詳細資訊，請參閱 AWS Config API 參考：<br>• DeleteResourceConfig<br>• PutResourceConfig | 2019 年 11 月 20 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 一致性套件 | 在此版本中， AWS Config 引入了一致性套件。一致性套件可讓您封裝規則集合和修正動作，然後可以將這些 AWS Config 規則集合一起部署為整個 AWS 組織中的單一實體。如需詳細資訊，請參閱 Conformance Packs。<br><br>如需 API 的詳細資訊，請參閱 AWS Config API 參考：<br><br>• DeleteOrganizationConformancePack<br>• DeleteOrganizationConformancePack<br>• DescribeConformance組合包<br>• DescribeConformance組合包<br>• DescribeConformancePackStatus<br>• DescribeOrganizationConformancePacks<br>• DescribeOrganizationConformancePack狀態<br>• GetConformancePackCompliance詳情<br>• GetConformancePackCompliance摘要<br>• GetOrganizationConformancePackDetailedStatus,<br>• PutConformance包<br>• PutOrganizationConformancePack | 2019 年 11 月 19 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 Amazon OpenSearch 服務和 AWS Key Management Service 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon OpenSearch 服務網域和 AWS Key Management Service 金鑰的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2019 年 11 月 11 日 |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br><br>• dms-replication-not-public<br>• emr-kerberos-enabled<br>• internet-gateway-authorized-vpc-only<br>• kms-cmk-not-scheduled-for-deletion<br>• sagemaker-notebook-no-direct-internet-access<br>• sagemaker-notebook-instance-kms-key-configured<br>• shield-drt-access<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2019 年 10 月 10 日 |
| AWS Config 支持 Amazon RDS 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫叢集和資料庫的組態變更。ClusterSnapshot<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2019 年 9 月 17 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 Amazon QLDB 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon Quantum Ledger Database (QLDB) 分類帳資源類型的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2019 年 9 月 10 日 |
| AWS Config 可讓您依 AWS Config 據規則評估，在不符合標準的資源上套用 auto 補救 | 在此版本中， AWS Config 引進了使用規則評估的不合 AWS Config 規資源上的 AWS Systems Manager 自動化文件套用自動補救的支援。如需詳細資訊，請參閱 使用規則修復不符合標準的資源 AWS Config。<br><br>在此版本中，新 AWS Config 增下列新 API。如需詳細資訊，請參閱 AWS Config API 參考：<br><br>• PutRemediation例外<br>• DescribeRemediation例外<br>• DeleteRemediation例外 | 2019 年 9 月 5 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 更新受管規則 | 在此發行版本中， AWS Config 支援下列受管規則：<br>• alb-http-to-https-redirection-check<br>• api-gw-cache-enabled-and-encrypted<br>• api-gw-endpoint-type-check<br>• cloudtrail-s3-dataevents-enabled<br>• cloudwatch-log-group-encrypted<br>• ebs-snapshot-public-restorable-check<br>• elb-deletion-protection-enabled<br>• lambda-concurrency-check<br>• lambda-dlq-check<br>• lambda-inside-vpc<br>• shield-advanced-enabled-autorenew<br>• vpc-vpn-2-tunnels-up<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2019 年 8 月 22 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 更新受管規則 | 在此發行版本中，會 AWS Config 更新下列受管規則：<br>• cloudfront-viewer-policy-https<br>• ec2-instance-no-public-ip<br>• ec2-security-group-attached-to-eni<br>• efs-encrypted-check<br>• elasticsearch-encrypted-at-rest<br>• elasticsearch-in-vpc-only<br>• redshift-cluster-public-access-check<br>• vpc-sg-open-only-to-authorized-ports<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2019 年 7 月 31 日 |
| AWS Config 支援 Amazon EC2 資源類型 | 在此版本中，您可以用 AWS Config 來記錄下列 Amazon EC2 資源的組態變更：vpcendPoint、VPC 和 V EndpointService PC。Peerin gConnection<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2019 年 7 月 12 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 可讓您管理組織 AWS 帳戶 內所有 AWS Config 規則 | 在此版本中， AWS Config 引入了管理組織 AWS 帳戶 內所有 AWS Config 規則的支援。您可以集中建立、更新和刪除組織中所有帳戶的 AWS Config 規則。如需詳細資訊，請參閱 管理組織中所有帳戶的 AWS Config 規則。<br><br>如需 API 的詳細資訊，請參閱 AWS Config API 參考：<br><br>• PutOrganizationConfigRule<br>• DescribeOrganizationConfigRules<br>• GetOrganizationConfigRuleDetailedStatus<br>• DescribeOrganizationConfigRule狀態<br>• DeleteOrganizationConfigRule | 2019 年 7 月 9 日 |
| AWS Config 支援 Amazon S3 和 Amazon EC2 資源類型 | 在此版本中，您可 AWS Config 以使用記錄對 Amazon S3 AccountPublicAccessBlock 資源和下列 Amazon EC2 資源的組態變更； NatGateway EgressOnlyInternetGateway、和 FlowLog。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2019 年 5 月 17 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 更新受管規則 | 在此發行版本中，會 AWS Config 更新下列受管規則：<br>• s3-bucket-public-read-prohibited<br>• s3-bucket-public-write-prohibited<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2019 年 5 月 7 日 |
| AWS Config 可讓您使用刪除修正動作 AWS Management Console。 | 在此版本中， AWS Config 引入了使用刪除補救動作的支援 AWS Management Console。如需詳細資訊，請參閱 使用規則修復不符合標準的資源 AWS Config。 | 2019 年 4 月 24 日 |
| AWS Config 支援新的受管規則 | 此版本支援新的受管規則：fms-shield-resource-policy-check。<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2019 年 4 月 7 日 |
| AWS Config 支援 Amazon API Gateway 資源類型 | 在此版本中，您可以用 AWS Config 來記錄下列 Amazon API Gateway 資源的組態變更：WebSocket API (API)、 RestApi (REST API)、階段 (WebSocket API 階段) 和階段 (REST API 階段)。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2019 年 3 月 20 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 可讓您執行進階查詢 | 在此版本中，可 AWS Config 新增根據資源組態屬性執行進階查詢的支援。如需詳細資訊，請參閱 查詢 AWS 資源目前的組態狀態。<br><br>在此版本中， AWS Config 新增 `SelectResourceConfig` API。有關更多信息，請參閱 AWS Config API 參考中的 SelectResourceConfig： | 2019 年 3 月 19 日 |
| AWS Config 允許您為 AWS Config 資源分配標籤 | 在此版本中， AWS Config 引入了三個 AWS Config 資源`ConfigRule`, `ConfigurationAggregator`, 和標籤式存取控制的支援`AggregationAuthorization` 。如需詳細資訊，請參閱 為您的 AWS Config 資源建立標籤。<br><br>在此版本中，您可以使用下列資料類型新增、移除或列出 AWS Config 資源的標籤。如需詳細資訊，請參閱 AWS Config API 參考：<br><br>• ListTagsForResource<br>• TagResource<br>• UntagResource | 2019 年 3 月 14 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 可讓您依 AWS Config 照規則評估，在不符合標準的資源上套用修正 | 在此版本中， AWS Config 引入了使用規則評估的不合 AWS Config 規資源上的 AWS Systems Manager 自動化文件套用補救的支援。如需詳細資訊，請參閱 使用規則修復不符合標準的資源 AWS Config。<br><br>在此版本中，新 AWS Config 增下列新 API。如需詳細資訊，請參閱 AWS Config API 參考：<br><br>• DeleteRemediation配置<br>• DescribeRemediation配置<br>• DescribeRemediationExecutionStatus<br>• PutRemediation配置<br>• StartRemediation執行 | 2019 年 3 月 12 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支持中國（寧夏）地區的 AWS Config 法規 | 此版本僅支援中國 (寧夏) 地區的 54 AWS Config 條規則。如需詳細資訊，請參閱 AWS Config 受管規則清單。<br><br>但是， AWS Config 目前在中國（寧夏）地區不支持以下規則：<br><br>• acm-certificate-expiration-check<br>• cmk-backing-key-rotation-enabled<br>• cloudformation-stack-drift-detection-check<br>• cloudformation-stack-notification-check<br>• cloud-trail-encryption-enabled<br>• cloud-trail-log-file-validation-enabled<br>• codebuild-project-envvar-awscred-check<br>• codebuild-project-source-repo-url-check<br>• codepipeline-deployment-count-check<br>• codepipeline-region-fanout-check<br>• dynamodb-table-encryption-enabled<br>• elb-acm-certificate-required<br>• encrypted-volumes<br>• fms-webacl-resource-policy-check<br>• fms-webacl-rulegroup-association-check<br>• guardduty-enabled-centralized | 2019 年 3 月 12 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| | • lambda-function-public-access-prohibited<br>• lambda-function-settings-check<br>• rds-storage-encrypted<br>• root-account-mfa-hardware-mfa-enabled<br>• root-account-mfa-enabled<br>• s3-bucket-blacklisted-actions-prohibited<br>• s3-bucket-policy-grantee-check<br>• s3-bucket-policy-not-more-p ermissive<br>• s3-bucket-public-read-prohibited<br>• s3-bucket-public-write-prohibited<br>• s3-bucket-server-side-encryption-enabled<br>• s3-bucket-ssl-requests-only | |
| AWS Config 支援新的受管規則 | 此版本支援下列新的受管規則：<br>• iam-user-mfa-enabled<br>• s3-bucket-policy-grantee-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2019 年 1 月 21 日 |
| AWS Config 支援 Service Catalog 資源類型 | 在此版本中，您可以用 AWS Config 來記錄下列 Service Catalog 資源 ( CloudFromation 產品、佈建產品及產品組合) 的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2019 年 1 月 11 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 服務連結 AWS Config 規則支援 | 在此版本中，新 AWS Config 增新的受管理組態規則，以支援其他 AWS 服務在您的帳戶中建立 AWS Config 規則。如需詳細資訊，請參閱 服務連結規 AWS Config 則。 | 2018 年 11 月 20 日 |
| AWS Config 可讓您彙總資源的組態 AWS 資料 | 在此版本中， AWS Config 引入了彙總 AWS 資源組態資料的支援。如需詳細資訊，請參閱 在彙總工具儀表板中檢視合規與庫存資料。<br><br>在此版本中，新 AWS Config 增下列新 API。如需詳細資訊，請參閱 AWS Config API 參考：<br><br>• BatchGetAggregateResourceConfig<br>• GetAggregateDiscoveredResource計數<br>• GetAggregateResourceConfig<br>• ListAggregateDiscoveredResources | 2018 年 11 月 19 日 |
| AWS Config 支援新的受管規則 | 此版本支援下列新的受管規則：<br><br>• cloudformation-stack-drift-detection-check<br>• codepipeline-deployment-count-check<br>• codepipeline-region-fanout-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2018 年 11 月 19 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的受管規則 | 此版本支援下列新的受管規則：<br>• access-keys-rotated<br>• cloud-trail-cloud-watch-logs-enabled<br>• cloud-trail-encryption-enabled<br>• cloud-trail-log-file-validation-enabled<br>• cmk-backing-key-rotation-enabled<br>• iam-policy-no-statements-with-admin-access<br>• iam-role-managed-policy-check<br>• iam-root-access-key-check<br>• iam-user-unused-credentials-check<br>• mfa-enabled-for-iam-console-access<br>• Amazon CloudWatch Logs<br>• root-account-hardware-mfa-enabled<br>• vpc-flow-logs-enabled<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2018 年 11 月 12 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的受管規則 | 此版本支援下列新的受管規則：<br>• dynamodb-table-encryption-enabled<br>• elb-logging-enabled<br>• rds-instance-public-access-check<br>• vpc-default-security-group-closed<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2018 年 10 月 24 日 |
| 合規歷史記錄的支援 | 透過此版本， AWS Config 現在支援根據 AWS Config Rules 評估的資源儲存符合性歷程記錄。如需詳細資訊，請參閱 檢視資源的合規歷史記錄時間軸。 | 2018 年 10 月 18 日 |
| 多帳戶多區域資料彙總區域支援 | 在此版本中，六個新區域現在皆支援多帳戶多區域資料彙整。如需詳細資訊，請參閱 Multi-Account Multi-Region Data Aggregation。 | 2018 年 10 月 4 日 |
| AWS Config 支援 AWS Config 規則 API 動作的資源層級權限 | 在此版本中， AWS Config 支援特定 AWS Config 規則 API 動作的資源層級權限。如需支援 API 的詳細資訊，請參閱AWS Config 規則 API 動作支援的資源層級權限。 | 2018 年 10 月 1 日 |
| AWS Config 支援 CodePipeline 資源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS CodePipeline 資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2018 年 9 月 12 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的受管規則 | 此版本支援下列新的受管規則：<br>• ec2-instance-managed-by-systems-manager<br>• ec2-managedinstance-association-compliance-status-check<br>• ec2-managedinstance-patch-compliance-status-check<br>• guardduty-enabled-centralized<br>• rds-snapshots-public-prohibited<br>• s3-bucket-blacklisted-actions-prohibited<br>• s3-bucket-policy-not-more-permissive<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2018 年 9 月 5 日 |
| AWS Config 支援 AWS Systems Manager 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 AWS Systems Manager 修補程式符合性和關聯符合性資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2018 年 8 月 9 日 |
| AWS Config 允許您刪除您的 AWS Config 數據 AWS Management Console | 在此版本中， AWS Config 引入了保留期使用的支援 AWS Management Console。在中 AWS Management Console，您可以為您選取自訂的資料保留期間`ConfigurationItems`。如需詳細資訊，請參閱 刪除 AWS Config 資料。 | 2018 年 8 月 7 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 AWS Shield 資源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS Shield 保護資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2018 年 8 月 7 日 |
| AWS Config 支持 AWS PrivateLink | 透過此版本提供 AWS Config 支援 AWS PrivateLink，讓您能夠在 Amazon Virtual Private Cloud (VPC) 之間以及 AWS Config 完全在網路內 AWS 路由資料。如需詳細資訊，請參閱 AWS Config 搭配使用介面 Amazon VPC 端點。 | 2018 年 7 月 31 日 |
| AWS Config 允許您刪除您的 AWS Config 數據 | 在此版本中， AWS Config 引入了保留期的支援。 AWS Config 允許您通過指定的保留期限來刪除您的數據`ConfigurationItems` 。如需詳細資訊，請參閱 刪除 AWS Config 資料。<br><br>在此版本中，新 AWS Config 增下列新 API。如需詳細資訊，請參閱 AWS Config API 參考：<br><br>• PutRetention配置<br>• DescribeRetention配置<br>• DeleteRetention配置 | 2018 年 5 月 25 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的受管規則 | 此版本支援下列兩種新的受管規則：<br>• lambda-function-settings-check<br>• s3-bucket-replication-enabled<br>• iam-policy-blacklisted-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2018 年 5 月 10 日 |
| AWS Config 支援 AWS X-Ray 資源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS X-Ray EncryptionConfig 資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2018 年 5 月 1 日 |
| AWS Config 支援 AWS Lambda 資源類型和一個新的受管規則 | 在此版本中，您可以使 AWS Config 用記錄對 AWS Lambda 函數資源類型的組態變更。如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本也支援 lambda-function-public-access-prohibited 受管規則。如需詳細資訊，請參閱 AWS Config 受管規則。 | 2018 年 4 月 25 日 |
| AWS Config 支援 AWS Elastic Beanstalk 資源類型 | 在此版本中，您可以用 AWS Config 來記錄對應用 AWS Elastic Beanstalk 程式、應用程式版本和環境資源的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2018 年 4 月 24 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的受管規則 | 此版本支援下列兩種新的受管規則：<br>• fms-webacl-resource-policy-check<br>• fms-webacl-rulegroup-association-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2018 年 4 月 4 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 多帳戶多區域資料彙整 | 在此版本中， AWS Config 引入了多帳戶多區域資料彙總。此功能可讓您將來自多個帳戶或一個組織和多個區域的 AWS Config 資料彙總至一個彙總帳戶。如需詳細資訊，請參閱 Multi-Account Multi-Region Data Aggregation。<br><br>在此版本中，新 AWS Config 增下列新 API。如需詳細資訊，請參閱 AWS Config API 參考：<br><br>• PutConfiguration聚合器<br>• DescribePendingAggregationRequests<br>• DeletePendingAggregationRequest<br>• PutAggregation授權<br>• DescribeAggregation授權<br>• GetAggregateConfigRuleComplianceSummary<br>• DescribeAggregateComplianceByConfigRules<br>• GetAggregateComplianceDetailsByConfig規則<br>• DescribeConfiguration聚合器<br>• DescribeConfigurationAggregatorSources狀態<br>• DeleteAggregation授權<br>• DeleteConfiguration聚合器 | 2018 年 4 月 4 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 使用 Amazon CloudWatch 事件監控 | 在此版本中，您可以使用 Amazon E CloudWatch vents 偵測 AWS Config 事件狀態的變更並做出回應。<br><br>如需詳細資訊，請參閱 AWS Config 使用 Amazon 監控 EventBridge。 | 2018 年 3 月 29 日 |
| 新的 API 操作 | 在此版本中， AWS Config 新增對 BatchGetResourceConfigAPI 的支援，讓您可以批次擷取一或多個資源的目前狀態。 | 2018 年 3 月 20 日 |
| AWS Config 支援 AWS WAF RuleGroup 資源類型 | 在此版本中，您可以使 AWS Config 用記錄 WAF RuleGroup 和 AWS W AWS AF RuleGroup 區域資源的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2018 年 2 月 15 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援新的受管規則 | 此版本支援下列新的受管規則：<br>• elb-acm-certificate-required<br>• elb-custom-security-policy-ssl-check<br>• elb-predefined-security-policy-ssl-check<br>• codebuild-project-envvar-awscred-check<br>• codebuild-project-source-repo-url-check<br>• iam-group-has-users-check<br>• s3-bucket-server-side-encryption-enabled<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2018 年 1 月 25 日 |
| AWS Config 支援 Elastic Load Balancing 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Elastic Load Balancing 傳統負載平衡器的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2017 年 11 月 17 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支持 Amazon CloudFront 和 AWS WAF 資源類型 | 在此版本中，您可以用 AWS Config 來記錄發 CloudFront 佈和串流散發的組態變更。<br><br>在此版本中，您可 AWS Config 以使用記錄下列資源 AWS WAF 和 AWS WAF 地區資源的組態變更；以費率為基礎的規則、規則和 Web ACL。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2017 年 11 月 15 日 |
| AWS Config 支持資 AWS CodeBuild 源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS CodeBuild 專案的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2017 年 10 月 20 日 |
| AWS Config 支援 Auto Scaling 資源和一個新的受管規則 | 在此版本中，您可以用 AWS Config 來記錄下列 Auto Scaling 資源的組態變更：群組、啟動設定、排程動作和擴展政策。<br><br>如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本也支援下列受管規則：<br><br>• autoscaling-group-elb-healthcheck-required<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2017 年 9 月 18 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支持資 AWS CodeBuild 源類型 | 在此版本中，您可以使 AWS Config 用記錄 AWS CodeBuild 專案的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2017 年 10 月 20 日 |
| AWS Config 支援 Auto Scaling 資源和一個新的受管規則 | 在此版本中，您可以用 AWS Config 來記錄下列 Auto Scaling 資源的組態變更：群組、啟動設定、排程動作和擴展政策。<br><br>如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本也支援下列受管規則：<br><br>• autoscaling-group-elb-healthcheck-required<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2017 年 9 月 18 日 |
| AWS Config 支援 DynamoDB 表格資源類型和一個新的受管規則 | 在此版本中，您可以使用 AWS Config 將組態變更記錄到 DynamoDB 表中。<br><br>如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本支援下列受管規則：<br><br>• dynamodb-autoscaling-enabled<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2017 年 9 月 8 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援兩個適用於 Amazon S3 的新受管規則 | 此版本支援兩項新的受管規則：<br>• s3-bucket-public-read-prohibited<br>• s3-bucket-public-write-prohibited<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2017 年 8 月 14 日 |
| AWS Config 控制台中的新頁面 | 您可以使用 AWS Config 控制台中的「儀表板」來查看以下內容：<br>• 資源總數<br>• 規則總數<br>• 不合規的資源數量<br>• 不合規的規則數量<br><br>如需詳細資訊，請參閱 檢視 AWS Config 儀表板。 | 2017 年 7 月 17 日 |
| 新的 API 操作 | 您可以使用此GetDiscoveredResourceCounts AWS Config 作業來傳回資源型態的數目、每種資源型態的數目，以及在「區域」中記錄的資源總數 AWS 帳戶。 | 2017 年 7 月 17 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 AWS CloudFormation 堆疊資源類型和一個新的受管規則 | 在此版本中，您可以用 AWS Config 來記錄 AWS CloudFormation 堆疊的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本支援下列受管規則：<br><br>• cloudformation-stack-notification-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2017 年 7 月 6 日 |
| 新的與更新的內容 | 此版本增加了對加拿大（中部）區域和南美洲（聖保羅）區域 AWS Config 規則的支援。<br><br>如需支援 AWS Config 和 Config 規則的所有區域 AWS 區域 ，請參閱 AWS 一般參考. | 2017 年 7 月 5 日 |
| 新的與更新的內容 | AWS Config 該 AWS GovCloud (US) 地區提供規則。如需詳細資訊，請參閱 AWS GovCloud (US) 使用者指南。<br><br>如需支援的區域 AWS Config，請參閱中的AWS 區域 和端點AWS 一般參考。 | 2017 年 6 月 8 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 Amazon CloudWatch 警示資源類型和三個新的受管規則 | 在此版本中，您可以用 AWS Config 來記錄 Amazon CloudWatch 警報的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本支援三項新的受管規則：<br><br>• cloudwatch-alarm-action-check<br>• cloudwatch-alarm-resource-check<br>• cloudwatch-alarm-settings-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2017 年 6 月 1 日 |
| 新的與更新的內容 | 此版本支援指定下列受管規則的應用程式版本號碼：<br><br>• ec2-managedinstance-applications-blacklisted<br>• ec2-managedinstance-applications-required<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2017 年 6 月 1 日 |
| 新的與更新的內容 | 此版本新增了對亞太區域 (孟買) 區域 AWS Config 規則的支援。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS 區域 與端點》。 | 2017 年 4 月 27 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 新的與更新的內容 | 此版本支援首次將 AWS Config 受管規則新增至您帳戶時的更新主控台體驗。<br><br>當您第一次設定 AWS Config 規則或在新區域中設定規則時，您可以依名稱、說明或標籤搜尋 AWS 受管規則。您可以選擇 Select all (全部新增) 選取所有規則，或是選擇 Clear all (全部清除) 清除所有規則。<br><br>如需詳細資訊，請參閱《新增、檢視、更新和刪除規則 (主控台)》。 | 2017 年 4 月 5 日 |
| AWS Config 支援新的受管規則 | 此版本支援下列新的受管規則：<br><br>• acm-certificate-expiration-check<br>• ec2-instance-detailed-monitoring-enabled<br>• ec2-managedinstance-inventory-blacklisted<br>• ec2-volume-inuse-check<br>• iam-user-group-membership-check<br>• iam-user-no-policies-check<br>• s3-bucket-ssl-requests-only<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2017 年 2 月 21 日 |
| 新的與更新的內容 | 此版本新增了對歐洲 (倫敦) 區域 AWS Config 規則的支援。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS 區域 與端點》。 | 2017 年 2 月 21 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 新的與更新的內容 | 此版 AWS CloudFormation 本新增 AWS Config 受管規則的範本。您可以使用範本建立您帳戶的受管規則。如需詳細資訊，請參閱 建立 AWS Config 受管規則 (使用 AWS CloudFormation 範本)。 | 2017 年 2 月 16 日 |
| 新的與更新的內容 | 此版本新增 `PutEvaluations` API 的新測試模式支援。在您的自訂規則中將 `TestMode` 參數設為 true 來驗證您的 AWS Lambda 函數是否會將評估結果交付至 AWS Config。您現有的評估不會有任何更新，評估結果也不會傳送到 AWS Config。<br><br>如需詳細資訊，請參閱 AWS Config API 參考PutEvaluations中的。 | 2017 年 2 月 16 日 |
| 新的與更新的內容 | 此版本新增了對亞太區域 (首爾) 和美國西部 (加利佛尼亞北部) 區域的 AWS Config 規則支援。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS 區域 與端點》。 | 2016 年 12 月 21 日 |
| 新的與更新的內容 | 此版本增加了對 AWS Config 歐洲（倫敦）地區的支持。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS 區域 與端點》。 | 2016 年 12 月 13 日 |
| 新的與更新的內容 | 此版本增加了對 AWS Config 加拿大（中部）區域的支持。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS 區域 與端點》。 | 2016 年 12 月 8 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 Amazon Redshift 資源類型和兩個新的受管規則 | 在此版本中，您可以用 AWS Config 來記錄 Amazon Redshift 叢集、叢集參數群組、叢集安全群組、叢集快照、叢集子網路群組和事件訂閱的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本支援兩項新的受管規則：<br><br>• redshift-cluster-configuration-check<br>• redshift-cluster-maintenancesettings-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2016 年 7 月 12 日 |
| 新的與更新的內容 | 此版本新增新受管規則的支援：<br><br>• dynamodb-throughput-limit-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2016 年 7 月 12 日 |
| 新的與更新的內容 | 此版本新增在帳戶中每個區域建立最多 50 條規則的支援。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS Config 限制》。 | 2016 年 7 月 12 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 Amazon EC2 系統管理員的受管執行個體庫存資源類型和三個新的受管規則 | 在此版本中，您可以使用 AWS Config 在代管執行個體上記錄軟體組態變更，並支援代管執行個體詳細目錄。<br><br>如需詳細資訊，請參閱 Recording Software Configuration for Managed Instances。<br><br>此版本支援三項新的受管規則：<br><br>• ec2-managedinstance-inventory-blacklisted<br>• ec2-managedinstance-applications-required<br>• ec2-managedinstance-platform-check<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2016 年 12 月 1 日 |
| AWS Config 支援 Amazon S3 儲存貯體資源和兩個新的受管規則 | 在此版本中，您可以用 AWS Config 來記錄 Amazon S3 儲存貯體的組態變更。如需詳細資訊，請參閱 支援的資源類型。<br><br>此版本支援兩項新的受管規則：<br><br>• s3-bucket-logging-enabled<br>• s3-bucket-versioning-enabled<br><br>如需詳細資訊，請參閱 AWS Config 受管規則。 | 2016 年 10 月 18 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 新的與更新的內容 | 此版本增加了對美國東部 (俄亥俄) 區域 AWS Config 和 AWS Config 規則的支援。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS 區域 與端點》。 | 2016 年 10 月 17 日 |
| 新的及更新的受管規則 | 此更新新增八項新受管規則的支援：<br>• approved-amis-by-id<br>• approved-amis-by-tag<br>• db-instance-backup-enabled<br>• desired-instance-type<br>• ebs-optimized-instance<br>• iam-password-policy<br>• rds-multi-az-support<br>• rds-storage-encrypted<br><br>您可以為下列規則指定多個參數值：<br>• desired-instance-tenancy<br>• required-tags<br><br>如需詳細資訊，請參閱 AWS Config 受管規則清單。 | 2016 年 10 月 4 日 |
| AWS Config 主機的新內容和更新內容 | 此更新新增了對在 AWS Config 時間軸中檢視 AWS CloudTrail API 活動的支援。如果您的帳戶 CloudTrail 正在記錄，您可以檢視建立、更新和刪除 API 事件，以便變更資源的設定。如需詳細資訊，請參閱 檢視組態和符合性歷程記。 | 2016 年 9 月 06 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 Elastic Load Balancing 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Elastic Load Balancing 應用程式負載平衡器的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2016 年 8 月 31 日 |
| 新的與更新的內容 | 此版本新增了對亞太區域 (新加坡) 和亞太區域 (雪梨) 區域的 AWS Config 規則支援。如需詳細資訊，請參閱《AWS 一般參考》中的《AWS 區域與端點》。 | 2016 年 8 月 18 日 |
| AWS Config 規則的新內容和更新內容 | 此更新新增建立可由組態變更觸發，同時也可以您選擇的定期頻率觸發之規則的支援。如需詳細資訊，請參閱 AWS Config 規則的評估模式與觸發程式型態。<br><br>此更新也新增了手動將您的資源與您的規則進行評估，以及刪除評估結果的支援。如需詳細資訊，請參閱 使用 AWS Config 規則評估您的資源。<br><br>此更新也新增了使用自訂規則評估其他資源類型的支援。如需詳細資訊，請參閱 評估其他資源類型。 | 2016 年 7 月 25 日 |
| AWS Config 支援 Amazon RDS 和 AWS Certificate Manager (ACM) 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫執行個體、資料庫安全群組、資料庫快照、資料庫子網路群組和事件訂閱的組態變更。您也可以使用 AWS Config 來記錄 ACM 提供之憑證的組態變更。<br><br>如需詳細資訊，請參閱 支援的資源類型。 | 2016 年 7 月 21 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 更新管理組態記錄器的相關資訊 | 此更新將重新命名及刪除組態記錄器的步驟新增至 管理組態記錄器。 | 2016 年 7 月 07 日 |
| 簡化角色建立及更新政策 | 透過此更新，可簡化為的 AWS Config 建立 IAM 角色。這項增強可在支援組態規則的區域中使用。為了支援這項增強，使用主控 AWS Config 台進行設定 中的步驟、適用於 AWS Config 交付通道的 Amazon S3 儲存貯體的許可 中的範例政策，以及以身分識別為基礎的原則範例 AWS Config 中的範例政策全部皆已更新。 | 2016 年 3 月 31 日 |
| 組態規則的範例函數和事件 | 此更新提供 AWS Config 規則的範例 AWS Lambda 函數 (Node.js) 中更新過的範例函數，並在 AWS Config 規則的範例事件 中新增了範例事件。 | 2016 年 3 月 29 日 |
| AWS Config 規則 GitHub 儲存庫 | 此更新會將有關AWS Config 規則 GitHub 存放庫的資訊新增至使用 AWS Config 規則評估資源。此儲存庫為使用者開發和貢獻的自訂規則提供範例函 AWS Config 數。 | 2016 年 3 月 1 日 |
| AWS Config 規則 | 此版本引入了 AWS Config 規則。透過規則，您可以用 AWS Config 來評估 AWS 資源是否符合您想要的組態。如需詳細資訊，請參閱 使用 AWS Config 規則評估資源。 | 2015 年 12 月 18 日 |
| AWS Config 支援 IAM 資源類型 | 在此版本中，您可以用 AWS Config 來記錄 IAM 使用者、群組、角色和客戶受管政策的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2015 年 12 月 10 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| AWS Config 支援 EC2 專用主機 | 在此版本中，您可以用 AWS Config 來記錄 EC2 專用主機的組態變更。如需詳細資訊，請參閱 支援的資源類型。 | 2015 年 23 月 11 日 |
| 更新許可資訊 | 此更新會新增下列 AWS 受管理原則的相關資訊 AWS Config：<br>• `AWS_ConfigRole` – 授予 AWS Config 許可，以取得有關您資源的組態詳細資訊。如需詳細資訊，請參閱 用以取得組態詳細資訊的 IAM 角色政策。<br>• `AWSConfigUserAccess` — 授與使用者的唯讀存取 AWS Config 權。如需詳細資訊，請參閱 唯讀存取權 AWS Config。 | 2015 年 10 月 19 日 |
| AWS Config 規則預覽 | 此版本介紹了 AWS Config 規則預覽。透過規則，您可以用 AWS Config 來評估 AWS 資源是否符合您想要的組態。如需詳細資訊，請參閱 使用 AWS Config 規則評估資源。 | 2015 年 10 月 7 日 |
| 新的與更新的內容 | 此版本增加了查找 AWS Config 已發現的資源的功能。如需詳細資訊，請參閱 查找發現的資源 AWS Config。 | 2015 年 8 月 27 日 |
| 新的與更新的內容 | 此版本新增了選取 AWS Config 記錄資源類型的功能。如需詳細資訊，請參閱 錄製 AWS 資源。 | 2015 年 6 月 23 日 |

| 變更 | 描述 | 版本日期 |
| --- | --- | --- |
| 新的與更新的內容 | 此版本為下列區域新增支援：亞太區域 (東京)、亞太區域 (新加坡)、歐洲 (法蘭克福)、南美洲 (聖保羅) 和美國西部 (加利佛尼亞北部)。如需詳細資訊，請參閱 AWS 區域 和端點。 | 2015 年 4 月 6 日 |
| 新指南 | 此版本推出 AWS Config。 | 2014 年 11 月 12 日 |

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。